

Docket No.: 56937-108

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
	:	
Hidenori NANKI, et al.	:	Confirmation Number:
	:	
Serial No.:	:	Group Art Unit:
	:	
Filed: January 27, 2004	:	Examiner: Unknown
	:	
For: INFORMATION PROCESSING APPARATUS	:	

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

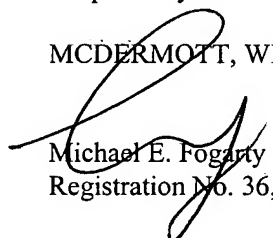
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-026810, filed February 4, 2003

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:tlb
Facsimile: (202) 756-8087
Date: January 27, 2004

56937-108
NANKI et al.
January 27, 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 4 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 2 6 8 1 0
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 2 6 8 1 0]

出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):

2 0 0 3 年 1 0 月 2 9 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 8 9 5 8 7

【書類名】 特許願

【整理番号】 5037740051

【あて先】 特許庁長官 殿

【国際特許分類】 G06B 9/06

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 南木 秀憲

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 吉岡 志郎

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 川口 謙一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 甲斐 俊也

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 深井 慎一郎

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100086737

【弁理士】

【氏名又は名称】 岡田 和秀

【電話番号】 06-6376-0857

【手数料の表示】

【予納台帳番号】 007401

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9305280

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置

【特許請求の範囲】

【請求項 1】 ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

CPUによる演算処理に用いられ、データの受け渡しを行い、その内部にデータを格納する機能を持つ汎用レジスタと、

前記汎用レジスタに付加され、前記ユーザメモリ空間から前記汎用レジスタのデータ部へのデータ転送が行われた場合はセキュリティ不要状態にセットされ、前記セキュアメモリ空間から前記汎用レジスタのデータ部にデータ転送が行われた場合はセキュリティ必要状態にセットされることが可能であるセキュア情報部と、

前記汎用レジスタのデータを前記ユーザメモリ空間に書き込む際に、前記セキュア情報部の値がセキュリティ必要状態かセキュリティ不要状態かを判別し、前記ユーザメモリ空間へのデータ転送を禁止するか否かの制御を行う機能を持つデータ制御部と、

前記アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、前記セキュア情報部の値を選択する機能を持つアドレス制御部とを備えることを特徴とする情報処理装置。

【請求項 2】 前記データ制御部から入力される命令コードを格納する際に、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、ユーザプログラムとセキュアプログラムのどちらが実行されているかを前記データ制御部に知らせる機能を持つ命令フェッチアドレス制御部と、

前記CPUによる命令フェッチ処理に用いられ、前記データ制御部から入力された命令コードをその内部に格納する機能を持つ命令バッファと、

前記ユーザメモリ空間上に配置されており、主にユーザによってプログラミングされるユーザプログラムと、

前記セキュアメモリ空間上に配置されており、主に開発者によってプログラミ

ングされ、ユーザにはその内容は非公開であるセキュアプログラムとを備え、

前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記命令フェッチアドレス制御部によって、前記ユーザメモリ空間から命令をフェッチしてきたことが判別された場合で、かつ、前記セキュア情報部の値がセキュリティ必要状態である場合、前記ユーザメモリ空間へのデータ転送を禁止することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記 CPU による演算処理に用いられ、前記データ制御部とデータの受け渡しを行い、その内部にデータを格納する機能を持つ複数の汎用レジスタと、

前記各汎用レジスタに付加されており、前記アドレス制御部の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態またはセキュリティ無効状態の値をセットすることが可能である複数のセキュア情報部と、

演算命令を実行して前記各汎用レジスタを用いて 2 つ以上のレジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも 1 つ以上含む場合は、演算結果を格納する汎用レジスタのセキュア情報部をセキュリティ無効状態とする機能を持つ汎用レジスタファイルとを備え、

前記データ制御部は、前記セキュア情報部がセキュリティ無効状態の汎用レジスタに対する演算命令を行う際に、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は演算を禁止することを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】 前記 CPU による演算処理に用いられ、比較演算処理等の結果を比較フラグとして値を保持する機能を持ち、演算命令を実行して、2 つ以上の汎用レジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも 1 つ以上含む場合で、かつ、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は、各フラグの値を変化させない状態レジスタを備えることを特徴とする請求項 2 に記載の情報処理装置。

【請求項5】 前記ユーザメモリ空間に外部からアクセスを行う際に使用される読み書き可能なI/O空間であるユーザI/O空間と、

前記セキュアメモリ空間に外部からアクセスを行う際に使用される読み書き可能なI/O空間であるセキュアI/O空間と、

前記セキュアI/O空間に接続して使用され、デバッグ鍵を含むデータを内部に格納する機能を持つICカードと、

前記ICカード内部に格納されており、開発者がユーザシステムで前記セキュアプログラムのデバッグを行う際に、前記セキュアI/O空間を介してCPUに読み出されると、前記命令フェッチアドレス制御部と前記アドレス制御部のアドレス判別機能を停止させる機能を持つデバッグ鍵とを備え、

前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記デバッグ鍵がCPUに読み出された場合には、前記ユーザメモリ空間と前記セキュアメモリ空間のどちらから命令をフェッチしてきた場合も前記ユーザメモリ空間へのデータ転送を禁止しない機能を持つことを特徴とする請求項2に記載の情報処理装置。

【請求項6】 ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータをCPU内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つセキュア情報付き内蔵RAM空間と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制

御を行うことを特徴とする情報処理装置。

【請求項 7】 ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をCPU内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つセキュア情報付き命令デコーダと、

前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つセキュア情報付き内蔵RAM空間と、

割り込み等の処理が発生した際に、前記セキュア情報付き内蔵RAM空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つセキュア情報付き割り込み退避情報部と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うことを特徴とする情報処理装置。

【請求項 8】 ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をCPU内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令

かを判別する機能を持つセキュア情報付き命令デコーダと、

前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つセキュア情報付き内蔵RAM空間と、

割り込み等の処理が発生した際に、前記セキュア情報付き内蔵RAM空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つセキュア情報付き割り込み退避情報部と、

前記セキュア情報付き内蔵RAM空間の一部をスタック領域に定義するスタックポインタと、

前記セキュア情報付き内蔵RAM空間のスタック領域の書き換え制御を行う退避情報書き換え制御部とを備え、

前記退避情報書き換え制御部は、前記セキュア情報付き命令デコーダの命令がユーザメモリ空間の命令でかつ前記セキュア情報付き内蔵RAM空間のスタック領域を書き換えようとした命令の場合には、その書き換えを禁止することを特徴とする情報処理装置。

【請求項 9】 ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

セキュア情報を保持する機能を持つセキュア情報付きDMAと、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータを前記セキュア情報付きDMA内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きDMAから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付きDMAに受け渡す機能を持つセキュア情報付き内蔵RAM空間と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付きDMAにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うことを特徴とする情報処理装置。

【請求項 10】 ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、

アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をCPU内部に受け渡すセキュア情報生成部と、

前記セキュア情報付きデータを受け取って保持する機能を持つセキュア情報付き汎用レジスタと、

実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つセキュア情報付き命令デコーダと、

前記セキュア情報付き命令デコーダでデコードされた命令により実行される演算に前記セキュア情報付き命令デコーダのセキュア情報を反映する機能を持つセキュア情報付き演算部と、

前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つデータ出力制御部とを備え、

前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報及び前記セキュア情報付き演算部にセットされた前記セキュア情報により前記外部空間へのデータ転送を禁止するか否かの制御を行うことを特徴とする情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置に関するものである。

【0002】

【従来の技術】

従来、例えばSDカードのセキュリティを守るのに、暗号解読をハードが行い、SDカード内の暗号データと暗号鍵とを用いて暗号を解読し、暗号化されていないデータに復号化していた。これが将来的には、複数の暗号化に対応するためにPDA (personal digital assistants: 携帯情報端末) 等でのコンテンツサー

ビスでは暗号解読をソフトで行うようになる可能性がある。従来は、OS (operatingsystem) の特権モードと通常モードでユーザがアクセスできる領域を切り分けることによって、また、メモリマネジメントユニット等のハードウェアのメモリ保護機能によって、暗号解読ソフトの外部漏洩を防いでいた。

【0003】

【特許文献1】

特開平6-266624号公報(第3-6頁、図1-図3)

【0004】

【発明が解決しようとする課題】

しかしながら、オープンソースなOSである例えばLinuxを使ったPDAでは、ソフトウェア開発環境が広くユーザに開示されることになる。これにより、アプリケーションの開発が行いやすくなる反面、Linux等の開示された開発環境で、ユーザがOSの持つ特権モードを利用して、ユーザモードではアクセスできないセキュリティのかけられた空間のデータを読み出し、ユーザRAM空間や外部空間への転送を行うことでOSのデバッグ作業を行っていたような従来技術を利用して、セキュリティ空間に置かれた暗号鍵やデータや命令を盗むといった悪用が簡単にできてしまう可能性があるという課題が出てくる。

【0005】

また、わが国では平成12年12月よりBSデジタル放送が開始され、放送のデジタル化が進むとともに、放送されたデジタルコンテンツの著作権が侵害される問題も発生している。そのため、放送コンテンツ提供者の中には、コンテンツを提供するに当たって厳格な著作権保護を求める者も現れており、放送メディアのデジタル化とデジタルコンテンツの円滑な流通を促進させるためには、放送コンテンツの権利保護のための何らかの措置が必要になってくる。

【0006】

本発明は、かかる点に鑑み、暗号解読アルゴリズムが明らかであってもオープンな開発環境に与えられる特権モードを利用するだけでは、セキュアメモリ空間の暗号鍵やデータや命令を読むことについて、これをできないようにすることで、将来的に行われる可能性の高い悪用を回避する情報処理装置を提供することを

目的とする。

【0007】

【課題を解決するための手段】

上記の課題を解決するために、本発明は次のような手段を講じる。

【0008】

(1) 第1の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～汎用レジスタ、セキュア情報部、データ制御部およびアドレス制御部を備えている。前記汎用レジスタは、CPUによる演算処理に用いられ、データの受け渡しを行い、その内部にデータを格納する機能を持つ。前記セキュア情報部は、前記汎用レジスタに付加され、前記ユーザメモリ空間から前記汎用レジスタのデータ部へのデータ転送が行われた場合はセキュリティ不要状態にセットされ、前記セキュアメモリ空間から前記汎用レジスタのデータ部にデータ転送が行われた場合はセキュリティ必要状態にセットされることが可能である。前記データ制御部は、前記汎用レジスタのデータを前記ユーザメモリ空間に書き込む際に、前記セキュア情報部の値がセキュリティ必要状態かセキュリティ不要状態かを判別し、前記ユーザメモリ空間へのデータ転送を禁止するか否かの制御を行う機能を持つ。前記アドレス制御部は、前記アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、前記セキュア情報部の値を選択する機能を持つ。

【0009】

上記構成による作用は次のとおりである。汎用レジスタにセキュア情報部である付加ビットを設けるだけで、CPUの命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュリティ空間からユーザ空間へのデータ複写を禁止することができる。すなわち、セキュアプログラムの解読（ハッキング）を防ぐことができる。

【0010】

(2) 第2の解決手段として、本発明による情報処理装置は、上記の第1の解

決手段において、さらに、それぞれ次のような機能を有する構成要素～命令フェッチアドレス制御部、命令バッファ、ユーザプログラムおよびセキュアプログラムを備えている。前記命令フェッチアドレス制御部は、前記データ制御部から入力される命令コードを格納する際に、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、ユーザプログラムとセキュアプログラムのどちらが実行されているかを前記データ制御部に知らせる機能を持つ。前記命令バッファは、前記CPUによる命令フェッチ処理に用いられ、前記データ制御部から入力された命令コードをその内部に格納する機能を持つ。前記ユーザプログラムは、前記ユーザメモリ空間上に配置されており、主にユーザによってプログラミングされるものである。前記セキュアプログラムは、前記セキュアメモリ空間上に配置されており、主に開発者によってプログラミングされ、ユーザにはその内容は非公開である。さらに、前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記命令フェッチアドレス制御部によって、前記ユーザメモリ空間から命令をフェッチしてきたことが判別された場合で、かつ、前記セキュア情報部の値がセキュリティ必要状態である場合、前記ユーザメモリ空間へのデータ転送を禁止するように構成されている。

【0011】

上記構成による作用は次のとおりである。開発者がセキュアメモリ空間でのセキュアプログラムの開発を行う場合には、ユーザメモリ空間とセキュアメモリ空間の領域間の自由なLOAD/STOREの特権を与えることができ、ユーザがユーザメモリ空間でのユーザプログラムの開発を行う場合には、セキュアメモリ空間からユーザメモリ空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムとユーザプログラムとで、セキュアメモリ空間のデータを自由に扱える権限の切り分けが可能である。

【0012】

(3) 第3の解決手段として、本発明による情報処理装置は、上記第2の解決手段において、さらに、それぞれ次のような機能を有する構成要素～複数の汎用レジスタ、複数のセキュア情報部および汎用レジスタファイルを備えている。前

記複数の汎用レジスタは、前記CPUによる演算処理に用いられ、前記データ制御部とデータの受け渡しを行い、その内部にデータを格納する機能を持つ。前記複数のセキュア情報部はそれぞれ、前記各汎用レジスタに付加されており、前記アドレス制御部の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態またはセキュリティ無効状態の値をセットすることが可能である。前記汎用レジスタファイルは、演算命令を実行して前記各汎用レジスタを用いて2つ以上のレジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも1つ以上含む場合は、演算結果を格納する汎用レジスタのセキュア情報部をセキュリティ無効状態とする機能を持つ。さらに、前記データ制御部は、前記セキュア情報部がセキュリティ無効状態の汎用レジスタに対する演算命令を行う際に、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は演算を禁止するように構成されている。

【0013】

上記構成による作用は次のとおりである。セキュアメモリ空間のデータを格納したレジスタの内容に対して、ユーザプログラムの演算処理による操作（例えば、セキュアメモリ空間からレジスタに読み出したデータと、オール“1”のデータとのAND演算を行った結果を、別のレジスタに格納するようなダミー演算などを行う操作）をできなくすることで、セキュアメモリ空間のメモリ内容の推測を防ぎ、セキュアプログラムの解読（ハッキング）を防ぐことができる。

【0014】

（4）第4の解決手段として、本発明による情報処理装置は、上記第2の解決手段において、さらに、次のような機能を有する状態レジスタを備えるものである。その状態レジスタは、前記CPUによる演算処理に用いられ、比較演算処理等の結果を比較フラグとして値を保持する機能を持ち、演算命令を実行して、2つ以上の汎用レジスタ同士の演算を行う際に、前記セキュア情報部の値がセキュリティ必要状態である前記汎用レジスタを少なくとも1つ以上含む場合で、かつ、前記命令フェッチアドレス制御部によって前記ユーザメモリ空間から演算命令をフェッチしてきたことが判別された場合は、各フラグの値を変化させないもの

である。

【0015】

上記構成による作用は次のとおりである。ユーザプログラムが、比較演算処理等の結果を比較フラグとして値を保持する状態レジスタを用いて2値以上のレジスタ比較を行ったとしても、セキュアメモリ空間のデータを格納したレジスタ内容の比較による推測を防ぎ、セキュアプログラムの解読を防ぐことができる。

【0016】

(5) 第5の解決手段として、本発明による情報処理装置は、上記第2の解決手段において、さらに、それぞれ次のような機能を有する構成要素～ユーザIO空間、セキュアIO空間、ICカードおよびデバッグ鍵を備えている。前記ユーザIO空間は、前記ユーザメモリ空間に外部からアクセスを行う際に使用される読み書き可能なIO空間である。前記セキュアIO空間は、前記セキュアメモリ空間に外部からアクセスを行う際に使用される読み書き可能なIO空間である。前記ICカードは、前記セキュアIO空間に接続して使用され、デバッグ鍵を含むデータを内部に格納する機能を持つ。前記デバッグ鍵は、前記ICカード内部に格納されており、開発者がユーザシステムで前記セキュアプログラムのデバッグを行う際に、前記セキュアIO空間を介してCPUに読み出されると、前記命令フェッチアドレス制御部と前記アドレス制御部のアドレス判別機能を停止させる機能を持つ。さらに、前記データ制御部は、転送命令を実行して前記汎用レジスタのデータ部からメモリ空間にデータ転送を実行する際に、前記デバッグ鍵がCPUに読み出された場合には、前記ユーザメモリ空間と前記セキュアメモリ空間のどちらから命令をフェッチしてきた場合も前記ユーザメモリ空間へのデータ転送を禁止しない機能を持つものに構成されている。

【0017】

上記構成による作用は次のとおりである。開発者がユーザシステムでセキュアプログラムのデバッグを行う際には、汎用レジスタのセキュア情報付加ビットの機能は停止され、ユーザメモリ空間とセキュアメモリ空間の領域間での自由なデータ転送が可能となり、セキュアプログラムをモニタリングできるようになる。すなわち、ユーザの環境においても、開発者はデバッグ鍵が格納されたICカー

ドによりセキュアプログラムを容易にデバッグでき、従来の特権モードと同義の権利を得られる。

【0018】

(6) 第6の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き内蔵RAM空間およびデータ出力制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータをCPU内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き内蔵RAM空間は、前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【0019】

上記構成による作用は次のとおりである。汎用レジスタにセキュア情報のための付加ビットを設けるだけで、CPUの命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュアメモリ空間から外部空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムの解読(ハッキング)を防ぐことができる。

【0020】

さらに、セキュア情報付き内蔵RAM空間を経由するデータのセキュリティ管理を可能とし、データ自身にセキュア情報を付加するため、内蔵RAM空間にセキュアメモリ空間のデータとユーザメモリ空間のデータの混在を可能とする。そ

して、ユーザメモリ空間の命令により、セキュア情報付き内蔵RAM空間上のセキュアデータの書き換えを許可し、通常使用に影響がない状態でセキュア情報付き内蔵RAM空間のセキュリティ管理を可能とすることができる。

【0021】

(7) 第7の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き命令デコーダ、セキュア情報付き内蔵RAM空間、セキュア情報付き割り込み退避情報部およびデータ出力制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をCPU内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き命令デコーダは、実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つ。前記セキュア情報付き内蔵RAM空間は、前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つ。前記セキュア情報付き割り込み退避情報部は、割り込み等の処理が発生した際に、前記セキュア情報付き内蔵RAM空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【0022】

上記構成による作用は次のとおりである。割り込み等によるセキュア情報付き内蔵RAM空間への退避データにセキュア情報を付加することにより、内蔵RAM空間に自動的に退避されたデータの読み出しにおけるセキュリティ管理を可能

にする。したがって、セキュアメモリ空間の重要なタスクのハッキングを防御することができる。

【0023】

(8) 第8の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き命令デコーダ、セキュア情報付き内蔵RAM空間、セキュア情報付き割り込み退避情報部、スタックポインタおよび退避情報書き換え制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をCPU内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き命令デコーダは、実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つ。前記セキュア情報付き内蔵RAM空間は、前記セキュア情報付き汎用レジスタから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付き汎用レジスタに受け渡す機能を持つ。前記セキュア情報付き割り込み退避情報部は、割り込み等の処理が発生した際に、前記セキュア情報付き内蔵RAM空間のスタック領域に退避するデータに前記セキュア情報付き命令デコーダの前記セキュア情報を付加する機能を持つ。前記スタックポインタは、前記セキュア情報付き内蔵RAM空間の一部をスタック領域に定義する。前記退避情報書き換え制御部は、前記セキュア情報付き内蔵RAM空間のスタック領域の書き換え制御を行う。さらに、前記退避情報書き換え制御部は、前記セキュア情報付き命令デコーダの命令がユーザメモリ空間の命令でかつ前記セキュア情報付き内蔵RAM空間のスタック領域を書き換えようとした命令の場合には、その書き換えを禁止するものである。

【0024】

上記構成による作用は次のとおりである。セキュアメモリ空間の命令実行中にユーザ割り込み等によって、セキュア情報付き内蔵RAM空間に退避されたセキ

ユーザメモリ空間への戻り先番地等を、ユーザメモリ空間の命令から書き換えることを禁止することにより、セキュアメモリ空間への正常な復帰を保証するとともに、ユーザメモリ空間の命令に許可されていないセキュアメモリ空間へのアクセスを制限し、なおかつ、前記セキュア情報付き内蔵RAM空間の通常領域とスタック領域を物理的に分割せずに、スタックポインタの指し示す空間による書き換え制御の切り替えでスタック領域のセキュリティ管理ができる。

【0025】

(9) 第9の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報付きDMA、セキュア情報生成部、セキュア情報付き内蔵RAM空間およびデータ出力制御部を備えている。前記セキュア情報付きDMAは、セキュア情報を保持する機能を持つ。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータを前記セキュア情報付きDMA内部に受け渡す。前記セキュア情報付き内蔵RAM空間は、前記セキュア情報付きDMAから前記セキュア情報付きデータを受け取って保持するとともに、前記保持したセキュア情報付きデータを前記セキュア情報付きDMAに受け渡す機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付きDMAにセットされた前記セキュア情報の値により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【0026】

上記構成による作用は次のとおりである。CPUが介在しないDMA転送データに対してもセキュア情報を追従させ、DMAを経由するデータのセキュリティ管理を可能とし、セキュアメモリ空間のデータ及び命令をセキュア情報付きDMAによりセキュア情報付き内蔵RAM空間に展開して使用する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能とし、セキュア情報付き内蔵RAM空間のデータ及び命令をセキュア情報付きDMAにより外部

空間に転送する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能にする。

【0027】

(10) 第10の解決手段として、本発明による情報処理装置は、ユーザメモリ空間とセキュアメモリ空間とからなるメモリ空間をアクセスする情報処理装置であって、それぞれ次のような機能を有する構成要素～セキュア情報生成部、セキュア情報付き汎用レジスタ、セキュア情報付き命令デコーダ、セキュア情報付き演算部およびデータ出力制御部を備えている。前記セキュア情報生成部は、アドレス情報が前記ユーザメモリ空間と前記セキュアメモリ空間のどちらを示しているかを判別し、セキュア情報を付加したデータ及び命令をCPU内部に受け渡す。前記セキュア情報付き汎用レジスタは、前記セキュア情報付きデータを受け取って保持する機能を持つ。前記セキュア情報付き命令デコーダは、実行中の命令が前記ユーザメモリ空間の命令か前記セキュアメモリ空間の命令かを判別する機能を持つ。前記セキュア情報付き演算部は、前記セキュア情報付き命令デコーダでデコードされた命令により実行される演算に前記セキュア情報付き命令デコーダのセキュア情報を反映する機能を持つ。前記データ出力制御部は、前記セキュア情報により外部空間へのデータ転送制御を行う機能を持つ。さらに、前記データ出力制御部は、前記セキュア情報付き汎用レジスタにセットされた前記セキュア情報及び前記セキュア情報付き演算部にセットされた前記セキュア情報により前記外部空間へのデータ転送を禁止するか否かの制御を行うように構成されている。

【0028】

上記構成による作用は次のとおりである。セキュアメモリ空間の命令であり、かつ、演算を行う命令を実行する場合、被演算対象となる全データがユーザメモリ空間のデータであっても、またはセキュア情報部にセキュアデータであることが明示されていなくても、セキュアメモリ空間の命令に付加されるセキュア情報をセキュア情報付き演算部のセキュア情報に反映することにより、演算結果が外部空間に流出することを防ぎ、演算結果からセキュアメモリ空間の命令内容を類推することを防御することができる。

【0029】**【発明の実施の形態】**

以下、本発明にかかわる情報処理装置の実施の形態を図面に基づいて説明する。

【0030】**(実施の形態1)**

図1は本発明の実施の形態1における情報処理装置の構成を示す概念図であり、図中、100は情報処理装置、101はCPU、102は汎用レジスタファイル、103は汎用レジスタ、104はセキュア情報部、105はデータ制御部、106はアドレス制御部、107はデータ／アドレスバス、110はユーザメモリ空間(RAM)、120はセキュアメモリ空間(ROM)である。このうち、情報処理装置100は装置の全体ブロックであり、外部にユーザメモリ空間110とセキュアメモリ空間120が接続されている。

【0031】

CPU101は、汎用レジスタファイル102を持ち、ユーザメモリ空間110とセキュアメモリ空間120にアクセスし、汎用レジスタ103へデータの読み書きを行う。汎用レジスタファイル102は、汎用レジスタ103とそれに対応したセキュア情報部104を持つ。汎用レジスタ103は、CPU101による演算処理に用いられ、データ制御部105とデータの受け渡しを行い、その内部にデータを格納する機能を持つ。セキュア情報部104は、汎用レジスタ103に付加されており、アドレス制御部106の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態の値をセットすることが可能である。

【0032】

データ制御部105は、データ／アドレスバス107から入力されたデータを汎用レジスタファイル102に書き込み、また汎用レジスタファイル102から受け取ったデータをデータ／アドレスバス107に出力してユーザメモリ空間110に書き込む際に、セキュア情報部104の値を判別して、書き込みを禁止するか否かの制御を行う機能を持つ。

【0033】

アドレス制御部106は、データ／アドレスバス107から入力されたアドレス情報がユーザメモリ空間110とセキュアメモリ空間120のどちらを示しているかを判別し、汎用レジスタファイル102内のセキュア情報部104の値を選択する機能を持つ。

【0034】

データ／アドレスバス107は、データ制御部105、アドレス制御部106、外部メモリデータバス130、外部メモリアドレスバス140を接続し、それぞれの間でのデータまたはアドレスの受け渡しを行う機能を持つ。

【0035】

ユーザメモリ空間110は、読み書き可能なメモリであり、外部メモリアドレスバス140から入力されたアドレス情報によって、外部メモリデータバス130とデータの入出力を行う機能を持つ。

【0036】

セキュアメモリ空間120は、読み出しのみが可能なメモリであり、外部メモリアドレスバス140から入力されたアドレス情報によって、外部メモリデータバス130にデータを出力する機能を持つ。

【0037】

外部メモリデータバス130は、情報処理装置100と、ユーザメモリ空間110またはセキュアメモリ空間120間のデータの受け渡しを行う機能を持つ。

【0038】

外部メモリアドレスバス140は、情報処理装置100から受け取ったアドレス情報をユーザメモリ空間110またはセキュアメモリ空間120に渡す機能を持つ。

【0039】

次に、上記のように構成された実施の形態1の情報処理装置の動作について説明する。

【0040】

図2は実施の形態1の動作を示すフローチャートであり、図中、601はLOAD命令発行処理、602はLOADアドレス判別処理、603はセキュリティ

必要処理、604はセキュリティ不要処理、605は汎用レジスタSTORE処理、606はSTORE命令発行処理、607はセキュリティ状態判別処理、608はユーザメモリ空間STORE処理、609はユーザメモリ空間STORE禁止処理である。

【0041】

LOAD命令発行処理601は、CPU101が外部メモリに対してLOAD命令を発行する処理であり、この処理を終えるとLOADアドレス判別処理602に移行する。

【0042】

LOADアドレス判別処理602は、アドレス制御部106がデータ／アドレスバス107から入力されたアドレス情報がセキュアメモリ空間120であるかそうでないかを判別し、セキュアメモリ空間120であるとき、セキュリティ必要処理603に移行し、そうでないとき（ユーザメモリ空間110であるとき）、セキュリティ不要処理604に移行する。

【0043】

セキュリティ必要処理603は、アドレス制御部106がセキュア情報部104の値をセキュリティ必要状態にセットする処理であり、この処理を終えると汎用レジスタSTORE処理605に移行する。

【0044】

セキュリティ不要処理604は、アドレス制御部106が、セキュア情報部104の値をセキュリティ不要状態にセットする処理であり、この処理を終えると汎用レジスタSTORE処理605に移行する。

【0045】

汎用レジスタSTORE処理605は、CPU101が、外部メモリから外部メモリデータバス130、データ／アドレスバス107、データ制御部105を介して受け取ったデータを汎用レジスタ103にストアする処理であり、この処理を終えるとSTORE命令発行処理606に移行する。

【0046】

STORE命令発行処理606は、CPU101が外部メモリに対してSTO

R E 命令を発行する処理であり、この処理を終えるとセキュリティ状態判別処理 607 に移行する。

【0047】

セキュリティ状態判別処理 607 は、データ制御部 105 がセキュア情報部 104 の値がセキュリティ不要状態であるかそうでないかを判別し、セキュリティ不要状態であるとき、ユーザメモリ空間 S T O R E 処理 608 に移行し、そうでないとき（セキュリティ必要状態であるとき）、ユーザメモリ空間 S T O R E 禁止処理 609 に移行する。

【0048】

ユーザメモリ空間 S T O R E 処理 608 は、C P U 101 が、汎用レジスタ 103 から受け取ったデータを、データ制御部 105、データ／アドレスバス 107、外部メモリデータバス 130 を介してユーザメモリ空間 110 にストアする処理であり、この処理を終えると動作完了である。

【0049】

ユーザメモリ空間 S T O R E 禁止処理 609 は、C P U 101 が、汎用レジスタ 103 から受け取ったデータを、データ制御部 105、データ／アドレスバス 107、外部メモリデータバス 130 を介してユーザメモリ空間 110 にストアすることを禁止する処理であり、この処理を終えると動作完了である。

【0050】

以上の構成により、レジスタにセキュア情報部である付加ビットを設けるだけで、C P U の命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュリティ空間からユーザ空間へのデータ複写を禁止することができる。すなわち、セキュアプログラムの解読（ハッキング）を防ぐことができるという格別の効果を奏する。

【0051】

（実施の形態 2）

上記の実施の形態 1 には次のような課題がある。すなわち、セキュアプログラムがセキュアメモリ空間で実行されている場合、例えば有料音楽配信サービスな

どで、配信されたMP3コンテンツをデコードし、デコードされたWAVEデータをユーザメモリ空間へ転送する、またはプログラム実行時に使用する関数の呼び出しを行い、必要なデータをユーザメモリ空間に一時的に退避しなければならない場合、セキュアメモリ空間からユーザメモリ空間へのデータ転送が発生する。このような場合にデータ転送を禁止すると、セキュアプログラムの動作内容が制限されるという課題が発生する。従って、ユーザプログラムによる転送であるのか、セキュアプログラムによる転送であるかの切り分けが可能となる新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態2である。以下、実施の形態2の情報処理装置の構成について説明する。

【0052】

図3は本発明の実施の形態2における情報処理装置の構成を示す概念図であり、図中、実施の形態1において説明した図1と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0053】

108は命令フェッチアドレス制御部、109は命令バッファ、110pはユーザプログラム、120pはセキュアプログラムである。

【0054】

このうち、命令フェッチアドレス制御部108は、命令バッファ109を持ち、データ制御部105から入力される命令コードを命令バッファ109に格納する際に、データ／アドレスバス107から入力されるアドレス情報がユーザメモリ空間110とセキュアメモリ空間120のどちらを示しているかを判別し、ユーザプログラム110pとセキュアプログラム120pのどちらが実行されているかをデータ制御部105に知らせる機能を持つ。

【0055】

命令バッファ109は、CPU101による命令フェッチ処理に用いられ、データ制御部105から入力された命令コードをその内部に格納する機能を持つ。

【0056】

ユーザプログラム110pは、ユーザメモリ空間110上に配置されており、主にユーザによってプログラミングされる。

【0057】

セキュアプログラム 120 p は、セキュアメモリ空間 120 上に配置されており、主に開発者によってプログラミングされ、ユーザにはその内容は非公開である。

【0058】

次に、上記のように構成された実施の形態 2 の情報処理装置の動作について説明する。

【0059】

図 4 は実施の形態 2 の動作を示すフローチャートであり、図中、実施の形態 1 において説明した図 2 と同様のフローについては、同一の番号を付し、その説明を省略する。

【0060】

701 は LOAD アドレス判別処理であり、命令フェッチアドレス制御部 108 が、データ／アドレスバス 107 から入力されたアドレス情報がセキュアメモリ空間 120 であるかそうでないかを判別し、セキュアメモリ空間 120 であるとき、ユーザメモリ空間 STORE 処理 608 に移行し、セキュアメモリ空間 120 でないとき、ユーザメモリ空間 STORE 禁止処理 609 に移行する。

【0061】

以上の構成により、開発者がセキュアメモリ空間でのセキュアプログラムの開発を行う場合には、ユーザメモリ空間とセキュアメモリ空間の領域間の自由な LOAD／STORE の特権を与えることができ、ユーザがユーザメモリ空間でのユーザプログラムの開発を行う場合には、セキュアメモリ空間からユーザメモリ空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムとユーザプログラムとで、セキュアメモリ空間のデータを自由に扱える権限の切り分けが可能であるという格別の効果を奏する。

【0062】**(実施の形態 3)**

上記の実施の形態 1 には、また次のような課題がある。すなわち、ユーザのプログラムによる汎用レジスタを介したセキュアメモリ空間からユーザメモリ空間

へのデータ転送を禁止することは可能であるが、例えば汎用レジスタ同士の演算を行った場合、その演算結果を新たなレジスタに格納してユーザメモリ空間にストアする行為は禁止されていない。例えば、セキュアメモリ空間からレジスタに読み出したデータと、オール“1”のデータとのAND演算を行った結果を、別のレジスタに格納するようなダミー演算を行うことで、セキュアメモリ空間のデータを容易に推測できるといった課題が発生する。従って、ユーザプログラムの演算に使用できるデータに制限をかけることが可能となる新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態3である。以下、実施の形態3の情報処理装置の構成について説明する。

【0063】

図5は本発明の実施の形態3における情報処理装置の構成を示す概念図であり、図中、実施の形態1、2において説明した図1、図3と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0064】

300は第1の汎用レジスタ、301は第2の汎用レジスタ、302は第3の汎用レジスタ、303は第1のセキュア情報部、304は第2のセキュア情報部、305は第3のセキュア情報部である。

【0065】

このうち、第1の汎用レジスタ300、第2の汎用レジスタ301、第3の汎用レジスタ302は、CPU101による演算処理に用いられ、データ制御部105とデータの受け渡しを行い、その内部にデータを格納する機能を持つ。

【0066】

第1のセキュア情報部303、第2のセキュア情報部304、第3のセキュア情報部305は、それぞれ第1の汎用レジスタ300、第2の汎用レジスタ301、第3の汎用レジスタ302に付加されており、アドレス制御部106の制御を受けて、セキュリティ必要状態またはセキュリティ不要状態またはセキュリティ無効状態の値をセットすることが可能である。

【0067】

次に、上記のように構成された実施の形態3の情報処理装置の動作について説

明する。

【0068】

図6は実施の形態3の動作を示すフローチャートであり、図中、実施の形態1、2において説明した図2、図4と同様のフローについては、同一の番号を付し、その説明を省略する。

【0069】

801は汎用レジスタ(1~2)STORE処理、802はCPU演算命令(1~2)発行処理、803はセキュリティ状態(1)判別処理、804はセキュリティ状態(2)判別処理、805はセキュリティ(3)無効処理、806はセキュリティ(3)不要処理、807は汎用レジスタ(3)演算結果格納処理、808はCPU演算命令(3)発行処理、809はセキュリティ状態(3)判別処理、810は演算禁止処理、811はCPUクリア命令(3)発行処理、812はセキュリティ(3)不要処理である。

【0070】

汎用レジスタ(1~2)STORE処理801は、CPU101が外部メモリから外部メモリデータバス130、データ/アドレスバス107、データ制御部105を介して受け取ったデータを第1の汎用レジスタ300、第2の汎用レジスタ301にストアする処理であり、この処理を終えるとCPU演算命令(1~2)発行処理802に移行する。

【0071】

CPU演算命令(1~2)発行処理802は、CPU101が第1の汎用レジスタ300、第2の汎用レジスタ301を用いて何らかの演算処理(ADD, SUBなど)を行う処理であり、この処理を終えるとセキュリティ状態(1)判別処理803に移行する。

【0072】

セキュリティ状態(1)判別処理803は、データ制御部105が第1のセキュリティ情報部303の値がセキュリティ必要状態であるかそうでないかを判別し、セキュリティ必要状態であるとき、セキュリティ(3)無効処理805に移行し、そうでないとき(セキュリティ不要状態であるとき)、セキュリティ状態(2

）判別処理 8 0 4 に移行する。

【 0 0 7 3 】

セキュリティ状態（2）判別処理 8 0 4 は、データ制御部 1 0 5 が第 2 のセキュア情報部 3 0 4 の値がセキュリティ必要状態であるかそうでないかを判別し、セキュリティ必要状態であるとき、セキュリティ（3）無効処理 8 0 5 に移行し、そうでないとき（セキュリティ不要状態であるとき）、セキュリティ（3）不要処理 8 0 6 に移行する。

【 0 0 7 4 】

セキュリティ（3）不要処理 8 0 6 は、アドレス制御部 1 0 6 が第 3 のセキュア情報部 3 0 5 の値をセキュリティ不要状態にセットする処理であり、この処理を終えると汎用レジスタ（3）演算結果格納処理 8 0 7 に移行する。

【 0 0 7 5 】

汎用レジスタ（3）演算結果格納処理 8 0 7 は、第 1 の汎用レジスタ 3 0 0、第 2 の汎用レジスタ 3 0 1 の演算処理結果を第 3 の汎用レジスタ 3 0 2 に格納する処理であり、この処理を終えると CPU 演算命令（3）発行処理 8 0 8 に移行する。

【 0 0 7 6 】

CPU 演算命令（3）発行処理 8 0 8 は、CPU 1 0 1 が第 3 の汎用レジスタ 3 0 2 を用いて何らかの演算処理（STORE, JUMP など）を行う処理であり、この処理を終えるとセキュリティ状態（3）判別処理 8 0 9 に移行する。

【 0 0 7 7 】

セキュリティ状態（3）判別処理 8 0 9 は、データ制御部 1 0 5 が第 3 のセキュア情報部 3 0 5 の値がセキュリティ無効状態であるかそうでないかを判別し、セキュリティ無効状態であるとき、演算禁止処理 8 1 0 に移行し、そうでないとき（セキュリティ不要状態またはセキュリティ必要状態であるとき）、CPU クリア命令（3）発行処理 8 1 1 に移行する。

【 0 0 7 8 】

CPU クリア命令（3）発行処理 8 1 1 は、CPU 1 0 1 が第 3 の汎用レジスタ 3 0 2 に対してクリア演算処理（CLR）を行う処理であり、この処理を終え

るとセキュリティ（３）不要処理 812 に移行する。

【0079】

セキュリティ（３）不要処理 812 は、アドレス制御部 106 が第 3 のセキュア情報部 305 の値をセキュリティ不要状態にセットする処理であり、この処理を終えると動作完了である。

【0080】

以上の構成により、セキュアメモリ空間のデータを格納したレジスタの内容に対して、ユーザプログラムの演算処理（ADD（＋），SUB（－），MUL（×），DIV（÷）などの四則演算）による操作をできなくすることで、セキュアメモリ空間のメモリ内容の推測を防ぐことができる。例えば、セキュアメモリ空間からレジスタに読み出したデータと、オール“1”のデータとのAND演算を行った結果を、別のレジスタに格納するようなダミー演算などを行うことで、セキュアメモリ空間のデータ推測（8' b11010011 & 8' b11111111 = 8' b11010011）、すなわち、セキュアプログラムの解読（ハッキング）を防ぐという格別の効果を奏する。

【0081】

（実施の形態 4）

上記の実施の形態 1 には、また次のような課題がある。すなわち、ユーザのプログラムによる 2 値以上のレジスタ比較を行った場合、演算結果を知らずとも、比較演算処理の結果を保持する状態レジスタを参照すれば、容易にセキュアメモリ空間のデータを推測できるといった課題が発生する。世の中に存在する多くの CPU では状態レジスタを持つものがほとんどであり、従って、ユーザプログラムの状態レジスタを用いた演算に制限をかける新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態 4 である。以下、実施の形態 4 の情報処理装置の構成について説明する。

【0082】

図 7 は本発明の実施の形態 4 における情報処理装置の構成を示す概念図であり、図中、実施の形態 1～3 において説明した図 1、図 3、図 5 と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0083】

400は状態レジスタであり、CPU101による演算処理に用いられ、比較演算処理等の結果を比較フラグとして値を保持する機能を持つ。

【0084】

次に、上記のように構成された実施の形態4の情報処理装置の動作について説明する。

【0085】

図8は実施の形態4の動作を示すフローチャートであり、図中、実施の形態1～3において説明した図2、図4、図6と同様のフローについては、同一の番号を付し、その説明を省略する。

【0086】

901は汎用レジスタ（1～2）比較演算処理、902は状態レジスタ比較フラグ変更禁止処理、903は状態レジスタ比較フラグ変更処理である。

【0087】

汎用レジスタ（1～2）比較演算処理901は、CPU101が第1の汎用レジスタ300、第2の汎用レジスタ301を用いて比較演算処理（CMPなど）を行う処理であり、この処理を終えるとセキュリティ状態（1）判別処理803に移行する。

【0088】

状態レジスタ比較フラグ変更禁止処理902は、汎用レジスタ（1～2）比較演算処理901の比較演算結果を受けて、状態レジスタ400の比較フラグの値を変更することを禁止する処理であり、この処理を終えると動作完了である。

【0089】

状態レジスタ比較フラグ変更処理903は、汎用レジスタ（1～2）比較演算処理901の比較演算結果を受けて、状態レジスタ400の比較フラグの値を変更する処理であり、この処理を終えると動作完了である。

【0090】

以上の構成により、ユーザプログラムが、比較演算処理等の結果を比較フラグとして値を保持する状態レジスタを用いて2値以上のレジスタ比較を行ったとし

でも、セキュアメモリ空間のデータを格納したレジスタ内容の比較による推測を防ぐことができる。すなわち、セキュアプログラムの解読を防ぐという格別の効果を奏する。

【0091】

(実施の形態5)

以上実施の形態1～4において、開発者がユーザシステムでセキュアプログラムのデバッグを行う際には、ユーザメモリ空間においてセキュアプログラムをモニタリングしなければならないので、セキュアメモリ空間からユーザメモリ空間へのデータ転送が禁止されているとデバッグできないといった課題が発生する。従って、レジスタを介したデータ転送を禁止する機能を解除する新たな機構を設ける必要がある。これの対策を講じるのが本発明の実施の形態5である。以下、実施の形態5の情報処理装置の構成について説明する。

【0092】

図9は本発明の実施の形態5における情報処理装置の構成を示す概念図であり、図中、実施の形態1～4において説明した図1、図3、図5、図7と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0093】

500は端末PC、501はユーザIO空間(RAM)、502はセキュアIO空間(RAM)、503はICカード、S503はデバッグ鍵である。

【0094】

このうち、端末PC500は、開発者によってセキュアプログラム120pのデバッグが行われる際に使用され、ユーザIO空間501に接続され、デバッグプログラムをユーザメモリ空間110に置いてデバッグを行う機能を持つ。

【0095】

ユーザIO空間501は、ユーザメモリ空間110に外部からアクセスを行う際に使用される読み書き可能なIO空間である。

【0096】

セキュアIO空間502は、セキュアメモリ空間120に外部からアクセスを行う際に使用される読み書き可能なIO空間である。

【0097】

ICカード503は、セキュアIO空間502に接続して使用され、デバッグ鍵S503等のデータを内部に格納する機能を持つ。

【0098】

デバッグ鍵S503は、ICカード503の内部に格納されており、開発者がユーザシステムでセキュアプログラム120pのデバッグを行う際に、セキュアIO空間502を介してCPU101に読み出されると、命令フェッチアドレス制御部108とアドレス制御部106のアドレス判別機能を停止させる機能を持つ。

【0099】

次に、上記のように構成された実施の形態5の情報処理装置の動作について説明する。

【0100】

図10は実施の形態5の動作を示すフローチャートであり、図中、実施の形態1～4において説明した図2、図4、図6、図8と同様のフローについては、同一の番号を付し、その説明を省略する。

【0101】

1001はデバッグ鍵入力処理、1002はデバッグ鍵LOAD処理、1003は命令フェッチアドレス制御部停止処理、1004はアドレス制御部停止処理である。

【0102】

デバッグ鍵入力処理1001は、ICカード503からセキュアIO空間502へデバッグ鍵S503を入力する処理であり、この処理を終えるとデバッグ鍵LOAD処理1002に移行する。

【0103】

デバッグ鍵LOAD処理1002は、CPU101が、セキュアIO空間502から外部メモリデータバス130、データ／アドレスバス107、データ制御部105を介してデバッグ鍵S503を読み出す処理であり、この処理を終えると命令フェッチアドレス制御部停止処理1003に移行する。

【0104】

命令フェッチアドレス制御部停止処理1003は、命令フェッチアドレス制御部108が持つアドレス判別機能を停止する処理であり、この処理を終えるとアドレス制御部停止処理1004に移行する。

【0105】

アドレス制御部停止処理1004は、アドレス制御部106が持つアドレス判別機能を停止する処理であり、この処理を終えるとLOAD命令発行処理601に移行する。

【0106】

以上の構成により、開発者がユーザシステムでセキュアプログラムのデバッグを行う際には、汎用レジスタのセキュア情報付加ビットの機能は停止され、ユーザメモリ空間とセキュアメモリ空間の領域間での自由なデータ転送が可能となり、セキュアプログラムをモニタリングできるようになる。すなわち、ユーザの環境においても、開発者はデバッグ鍵が格納されたICカードにより、セキュアプログラムを容易にデバッグでき、従来の特権モードと同義の権利を得られる、という格別の効果を奏する。

【0107】

(実施の形態6)

図11は本発明の実施の形態6における情報処理装置の構成を示す概念図である。本実施の形態の情報処理装置は、セキュアメモリ空間201と、ユーザメモリ空間202と、データバス203と、アドレスバス204と、セキュア情報生成部205と、セキュア情報付き内蔵RAM空間206と、CPU208と、セキュア情報付き汎用レジスタ209と、データ出力制御部211と、外部空間212とによって構成されている。

【0108】

さらに、図12(a)，(b)に示すように、セキュア情報付き内蔵RAM空間206は内部にセキュア情報部207を備え、セキュア情報付き汎用レジスタ209は内部にセキュア情報部210を備えている。

【0109】

CPU 208は、セキュアメモリ空間201またはユーザメモリ空間202のデータを読み出す際にアドレスバス204を通じてアドレスを指定する。

【0110】

セキュアメモリ空間201またはユーザメモリ空間202は、アドレスバス204で指定されたアドレス情報に従いデータを出力する。

【0111】

セキュア情報生成部205は、指定したアドレス情報に合致したデータを受け取り、指定したアドレス情報がユーザメモリ空間202とセキュアメモリ空間201のどちらを示しているかを判別し、ユーザメモリ空間202のデータである場合にはセキュア情報として“0”を、セキュアメモリ空間201のデータである場合にはセキュア情報として“1”を付加したデータをセキュア情報付き汎用レジスタ209に受け渡す。セキュア情報はセキュア情報付き汎用レジスタ209内のセキュア情報部210に格納される。

【0112】

セキュア情報付き汎用レジスタ209のデータをセキュア情報付き内蔵RAM空間206と外部空間212に転送する場合の動作を、図13(a), (b)を用いて説明する。

【0113】

206aはセキュア情報付き内蔵RAM空間206の第1の状態であり、206bはRAM空間206の第2の状態であり、207aはセキュア情報部207の第1の状態であり、207bはセキュア情報部207の第2の状態であり、209aは汎用レジスタ209の第1の状態であり、209bは汎用レジスタ209の第2の状態であり、210aはセキュア情報部210の第1の状態であり、210bはセキュア情報部210の第2の状態である。

【0114】

CPU 208が汎用レジスタ209の第1の状態209aのデータをセキュア情報付き内蔵RAM空間206の第1の状態206aに書き込むと同時に、セキュア情報部210の第1の状態210aの値はセキュア情報部207の第1の状態207aに書き込まれ、セキュア情報付き内蔵RAM空間206の第2の状態

2 0 6 b とセキュア情報部 2 0 7 の第 2 の状態 2 0 7 b となり、セキュア情報は保持される。

【0 1 1 5】

C P U 2 0 8 がセキュア情報付き内蔵 R A M 空間 2 0 6 の第 2 の状態 2 0 6 b のデータを読み出すと、汎用レジスタ 2 0 9 の第 2 の状態 2 0 9 b にデータが受け渡されると同時に、セキュア情報部 2 0 7 の第 2 の状態 2 0 7 b はセキュア情報部 2 1 0 の第 2 の状態 2 1 0 b に受け渡され、セキュア情報付き内蔵 R A M 空間 2 0 6 を経由するデータのセキュア情報は保持される。

【0 1 1 6】

C P U 2 0 8 が外部空間 2 1 2 にセキュア情報付き汎用レジスタ 2 0 9 のデータを出力する際に、データ出力制御部 2 1 1 は、セキュア情報付き汎用レジスタ 2 0 9 内のセキュア情報部 2 1 0 の値が“1”である場合には外部空間 2 1 2 へのデータ出力を禁止する。

【0 1 1 7】

以上の構成により、レジスタに付加ビットを設けるだけで、C P U の命令セットを変更することなく、また、特権モードと通常モードの切り替え制御を行わずして、ユーザのプログラムによるレジスタを介したセキュアメモリ空間から外部空間へのデータ転送を禁止することができる。すなわち、セキュアプログラムの解読(ハッキング)を防ぐことができる。

【0 1 1 8】

さらに内蔵 R A M 空間に対してもセキュア情報を追従させ、内蔵 R A M 空間を経由するデータのセキュリティ管理を可能とし、データ自身にセキュア情報を付加するために、内蔵 R A M 空間にセキュアメモリ空間のデータとユーザメモリ空間のデータの混在を可能とし、ユーザメモリ空間の命令により、セキュア情報付き内蔵 R A M 空間上のセキュアデータの書き換えを許可し、通常使用に影響がない状態でセキュア情報付き内蔵 R A M 空間のセキュリティ管理を可能とすることができるという格別の効果を奏する。

【0 1 1 9】

(実施の形態 7)

図 14 は本発明の実施の形態 7 における情報処理装置の構成を示す概念図であり、図中、実施の形態 6 において説明した図 11 と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0120】

図 14 において、213 は割り込み制御部、214 はセキュア情報付き割り込み退避情報部、216 はセキュア情報付き命令デコーダ 216 である。

【0121】

図 15 (a), (b) に示すように、セキュア情報付き割り込み退避情報部 214 は内部にセキュア情報部 215 を備え、セキュア情報付き命令デコーダ 216 は内部にセキュア情報部 217 を備える。

【0122】

CPU 208 は、セキュアメモリ空間 201 またはユーザメモリ空間 202 のデータリード及び命令フェッチを行う際に、アドレスバス 204 を通じてアドレスを指定する。

【0123】

セキュアメモリ空間 201 またはユーザメモリ空間 202 は、アドレスバス 204 で指定されたアドレス情報に従いデータ及び命令を出力する。

【0124】

セキュア情報生成部 205 は、指定したアドレス情報に合致したデータ及び命令を受け取り、指定したアドレス情報がユーザメモリ空間 202 とセキュアメモリ空間 201 のどちらを示しているかを判別し、ユーザメモリ空間 202 のデータである場合にはセキュア情報として“0”を、セキュアメモリ空間 201 のデータである場合にはセキュア情報として“1”を付加したデータをセキュア情報付き汎用レジスタ 209 に受け渡し、セキュア情報はセキュア情報付き汎用レジスタ 209 内のセキュア情報部 210 (図 12 参照) に格納される。

【0125】

ユーザメモリ空間 202 の命令である場合にはセキュア情報として“0”を、セキュアメモリ空間 201 の命令である場合にはセキュア情報として“1”を付加した命令をセキュア情報付き命令デコーダ 216 に受け渡し、セキュア情報は

セキュア情報部 2 1 7 に格納される。

【 0 1 2 6 】

セキュア情報付き汎用レジスタ 2 0 9 のデータを、セキュア情報付き内蔵 R A M 空間 2 0 6 に転送する場合の動作は、実施の形態 6 において説明した内容と同様であるため、その説明を省略する。

【 0 1 2 7 】

割り込み制御部 2 1 3 により割り込み等の処理が発生した際に、セキュア情報付き内蔵 R A M 空間 2 0 6 の一部に自動的に退避するデータに対しセキュリティ管理を行うために、現在実行中の命令がユーザメモリ空間 2 0 2 とセキュアメモリ空間 2 0 1 のどちらの命令かによって、退避するデータにセキュア情報を付加する。

【 0 1 2 8 】

現在実行中の命令は、セキュア情報付き命令デコーダ 2 1 6 内のセキュア情報部 2 1 7 の値で判別可能であり、ユーザメモリ空間 2 0 2 の命令である場合にはセキュア情報は“0”であり、セキュアメモリ空間 2 0 1 の命令である場合にはセキュア情報は“1”である。

【 0 1 2 9 】

割り込み発生時に自動的に退避される情報がセキュア情報であるかどうかを明示するため、セキュア情報付き割り込み退避情報部 2 1 4 内のセキュア情報部 2 1 5 にセキュア情報付き命令デコーダ 2 1 6 内のセキュア情報部 2 1 7 の値を伝搬させる。

【 0 1 3 0 】

さらに、セキュア情報付き割り込み退避情報部 2 1 4 のデータをセキュア情報付き内蔵 R A M 空間 2 0 6 の一部に退避すると同時に、セキュア情報付き割り込み退避情報部 2 1 4 内のセキュア情報部 2 1 5 の値をセキュア情報付き内蔵 R A M 空間 2 0 6 内のセキュア情報部 2 0 7 (図 1 2 参照) に伝搬させる。これにより、退避するデータのセキュア情報は保持される。

【 0 1 3 1 】

セキュア情報付き内蔵 R A M 空間 2 0 6 のデータをセキュア情報付き汎用レジ

スタ 209 に転送する場合の動作は、実施の形態 6 において説明した内容と同様であるため、その説明を省略する。

【0132】

CPU 208 が外部空間 212 にセキュア情報付き汎用レジスタ 209 のデータを出力する際に、データ出力制御部 211 は、セキュア情報付き汎用レジスタ 209 内のセキュア情報部 210 の値が“1”である場合には外部空間 212 へのデータ出力を禁止する。

【0133】

以上の構成により、割り込み等によるスタック退避情報にもセキュア情報を付加追従させ、セキュア情報付き内蔵 RAM 空間の一部であるスタック領域に自動的に退避されたデータの読み出しにおけるセキュリティ管理を可能とし、例えば、セキュアメモリ空間の命令実行中の実行 PC（プログラムカウンタ）等が外部空間に読み出されることから起こり得る、セキュアメモリ空間の重要なタスクのハッキングを防御することができるという格別の効果を奏する。

【0134】

（実施の形態 8）

図 16 は本発明の実施の形態 8 における情報処理装置の構成を示す概念図であり、図中、実施の形態 6、7 において説明した図 11、図 14 と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0135】

図 16 において、218 はスタックポインタ、219 は退避情報書き換え制御部である。

【0136】

CPU 208 は、セキュアメモリ空間 201 またはユーザメモリ空間 202 のデータリード及び命令フェッチを行う際に、アドレスバス 204 を通じてアドレスを指定する。

【0137】

セキュアメモリ空間 201 またはユーザメモリ空間 202 は、アドレスバス 204 で指定されたアドレス情報に従いデータ及び命令を出力する。

【0138】

セキュア情報生成部205は、指定したアドレス情報に合致したデータ及び命令を受け取り、指定したアドレス情報がユーザメモリ空間202とセキュアメモリ空間201のどちらを示しているかを判別し、ユーザメモリ空間202のデータである場合にはセキュア情報として“0”を、セキュアメモリ空間201のデータである場合にはセキュア情報として“1”を付加したデータをセキュア情報付き汎用レジスタ209に受け渡し、セキュア情報はセキュア情報付き汎用レジスタ209内のセキュア情報部210（図12参照）に格納される。また、セキュア情報生成部205は、ユーザメモリ空間202の命令である場合にはセキュア情報として“0”を、セキュアメモリ空間201の命令である場合にはセキュア情報として“1”を付加した命令をセキュア情報付き命令デコーダ216に受け渡し、セキュア情報はセキュア情報付き命令デコーダ216内のセキュア情報部217（図15参照）に格納される。

【0139】

割り込み制御部213により割り込み等の処理が発生した際に、セキュア情報付き内蔵RAM空間206のスタックポインタ218の指し示すスタック領域に自動的に退避するデータに対しセキュリティ管理を行うために、現在実行中の命令がユーザメモリ空間202とセキュアメモリ空間201のどちらの命令かによって、退避するデータにセキュア情報を付加する場合の動作は、実施の形態7において説明した内容と同様であるため、その説明を省略する。

【0140】

また、セキュア情報付き内蔵RAM空間206の通常領域及びスタック領域のデータをセキュア情報付き汎用レジスタ209に転送する場合の動作は、実施の形態6において説明した内容と同様であるため、その説明を省略する。

【0141】

以上の構成により、割り込み等によるスタック退避情報にもセキュア情報を付加追従させ、セキュア情報付き内蔵RAM空間の一部であるスタック領域に自動的に退避されたデータの読み出しにおけるセキュリティ管理を可能とする。

【0142】

また、セキュア情報付き汎用レジスタ 209 のデータを、セキュア情報付き内蔵 RAM 空間 206 の通常領域に転送（ライト）する場合の動作は、実施の形態 6 において説明した内容と同様であるため、その説明を省略する。

【0143】

また、セキュア情報付き汎用レジスタ 209 のデータを、セキュア情報付き内蔵 RAM 空間 206 のスタック領域に転送（ライト）する場合、退避情報書き換え制御部 219 は、現在実行中の命令がユーザメモリ空間 202 とセキュアメモリ空間 201 のどちらかをセキュア情報付き命令デコーダ 216 内のセキュア情報部 217（図 15 参照）の値により判別し、さらに転送する空間のアドレスとスタックポインタ 218 を比較し、ユーザメモリ空間 202 の命令であり、かつスタック領域への転送であった場合には、データの転送を禁止する。

【0144】

さらに、セキュア情報付き内蔵 RAM 空間 206 の一部であるスタック領域へのデータの退避及び復帰における動作を、図 17（a），（b）を用いて説明する。

【0145】

206c はセキュア情報付き内蔵 RAM 空間 206 の第 1 の状態であり、206d は RAM 空間 206 の第 2 の状態であり、207c はセキュア情報部 207 の第 1 の状態であり、218c はスタックポインタ 218 の第 1 の状態であり、218d はスタックポインタ 218 の第 2 の状態であり、701c はスタック領域の第 1 の状態であり、701d はスタック領域の第 2 の状態であり、702c は通常領域の第 1 の状態であり、702d は通常領域の第 2 の状態であり、703c はスタック退避情報である。

【0146】

セキュア情報付き内蔵 RAM 空間 206 の第 2 の状態 206d を初期状態とする。セキュアメモリ空間 201 の命令実行中に割り込みが発生し、ユーザメモリ空間 202 の処理へ移行する場合、セキュア情報付き割り込み退避情報部 214 のデータがセキュア情報付き内蔵 RAM 空間 206 の第 2 の状態 206d に退避され、その結果、RAM 空間 206 の第 1 の状態 206c 中のスタック退避情報

703cになる。

【0147】

この状態では、スタック退避情報にセキュア情報が付加されているため、スタック退避されたデータの読み出しにおけるセキュリティ管理を可能とし、また、スタック領域の第1の状態701cは退避情報書き換え制御部219によりユーザメモリ空間202の命令では書き換えを禁止しているため、スタック退避されたデータの書き込みにおけるセキュリティ管理を可能とする。

【0148】

割り込みからの復帰によりスタック退避情報703cが復帰すると、スタックポインタの第1の状態218cはスタックポインタの第2の状態218dとなり、不必要となったスタック退避情報703cの領域を通常領域の第1の状態702cに開放され、通常領域の第2の状態702dとなる。

【0149】

以上の構成により、セキュアメモリ空間の命令実行中にユーザ割り込み等によって、セキュア情報付き内蔵RAM空間に退避されたセキュアメモリ空間への戻り先番地等を、ユーザメモリ空間の命令から書き換えることを禁止することにより、セキュアメモリ空間への正常な復帰を保証するとともに、ユーザメモリ空間の命令に許可されていないセキュアメモリ空間へのアクセスを制限し、なおかつ、前記セキュア情報付き内蔵RAM空間の通常領域とスタック領域を物理的に分割せずに、スタックポインタの指し示す空間による書き換え制御の切り替えでスタック領域のセキュリティ管理ができるという格別の効果を奏する。

【0150】

(実施の形態9)

図18は本発明の実施の形態9における情報処理装置の構成を示す概念図であり、図中、実施の形態6において説明した図11と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0151】

図18において、220はセキュア情報付きDMAである。図19に示すように、セキュア情報付きDMA220はその内部にセキュア情報部221を備えて

いる。

【0 1 5 2】

セキュア情報付きDMA 2 2 0 はセキュアメモリ空間 2 0 1 またはユーザメモリ空間 2 0 2 からのデータ転送を行う際に、アドレスバス 2 0 4 を通じてアドレスを指定する。

【0 1 5 3】

セキュアメモリ空間 2 0 1 またはユーザメモリ空間 2 0 2 は、アドレスバス 2 0 4 で指定されたアドレス情報に従いデータを出力する。

【0 1 5 4】

セキュア情報生成部 2 0 5 は、指定したアドレス情報に合致したデータを受け取り、指定したアドレス情報がユーザメモリ空間 2 0 2 とセキュアメモリ空間 2 0 1 のどちらを示しているかを判別し、ユーザメモリ空間 2 0 2 のデータである場合にはセキュア情報として“0”を、セキュアメモリ空間 2 0 1 のデータである場合にはセキュア情報として“1”を付加したデータをセキュア情報付きDMA 2 2 0 に受け渡す。セキュア情報はセキュア情報付きDMA 2 2 0 内のセキュア情報部 2 2 1 に格納される。

【0 1 5 5】

セキュア情報付きDMA 2 2 0 のデータを、セキュア情報付き内蔵RAM空間 2 0 6 と外部空間 2 1 2 に転送する場合の動作は、実施の形態 6 において説明した内容と同様であるため、その説明を省略する。

【0 1 5 6】

また、セキュア情報付きDMA 2 2 0 は、セキュア情報付き内蔵RAM空間 2 0 6 からのデータ転送を行う際に、アドレスバス 2 0 4 を通じてアドレスを指定する。

【0 1 5 7】

セキュア情報付き内蔵RAM空間 2 0 6 は、アドレスバス 2 0 4 で指定されたアドレス情報に従いセキュア情報部 2 0 7 (図 1 2 参照) のセキュア情報を付加したデータを出力する。

【0 1 5 8】

セキュア情報付きDMA 220は、指定したアドレス情報に合致したデータを受け取ると同時に、セキュア情報部207のセキュア情報をセキュア情報部221に反映させることにより、セキュア情報付きDMA 220を経由するデータのセキュア情報は保持される。

【0159】

以上の構成により、CPUが介在しないDMA転送データに対してもセキュア情報を追従させ、DMAを経由するデータのセキュリティ管理を可能とし、セキュアメモリ空間のデータ及び命令をセキュア情報付きDMAによりセキュア情報付き内蔵RAM空間に展開して使用する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能とし、セキュア情報付き内蔵RAM空間のデータ及び命令をセキュア情報付きDMAにより外部空間に転送する場合においても、セキュアメモリ空間のデータ及び命令のセキュリティ管理を可能とするという格別の効果を奏する。

【0160】

(実施の形態10)

図20は本発明の実施の形態10における情報処理装置の構成を示す概念図であり、図中、実施の形態6において説明した図11と同様のブロックについては、同一の番号を付し、その説明を省略する。

【0161】

図20において、216はセキュア情報付き命令デコーダ、222はセキュア情報付き演算部である。図21に示すように、セキュア情報付き演算部222は内部にセキュア情報部223を備えている。

【0162】

CPU 208は、セキュアメモリ空間201またはユーザメモリ空間202のデータリード及び命令フェッチを行う際に、アドレスバス204を通じてアドレスを指定する。

【0163】

セキュアメモリ空間201またはユーザメモリ空間202は、アドレスバス204で指定されたアドレス情報に従いデータ及び命令を出力する。

【0164】

セキュア情報生成部205は、指定したアドレス情報に合致したデータ及び命令を受け取り、指定したアドレス情報がユーザメモリ空間202とセキュアメモリ空間201のどちらを示しているかを判別し、ユーザメモリ空間202のデータである場合にはセキュア情報として“0”を、セキュアメモリ空間201のデータである場合にはセキュア情報として“1”を付加したデータをセキュア情報付き汎用レジスタ209に受け渡し、セキュア情報はセキュア情報付き汎用レジスタ209内のセキュア情報部210（図12参照）に格納される。また、セキュア情報生成部205は、ユーザメモリ空間202の命令である場合にはセキュア情報として“0”を、セキュアメモリ空間201の命令である場合にはセキュア情報として“1”を付加した命令をセキュア情報付き命令デコーダ216に受け渡し、セキュア情報はセキュア情報付き命令デコーダ216内のセキュア情報部217（図15参照）に格納される。

【0165】

セキュアメモリ空間201の演算命令がセキュア情報付き命令デコーダ216によりデコードされた結果を受け、セキュア情報付き汎用レジスタ209のデータがセキュア情報付き演算部222に受け渡され、セキュア情報付き演算部222は演算を開始する。

【0166】

このとき、被演算対象となる1つ以上のセキュア情報付き汎用レジスタ209のデータに付加されるセキュア情報部210のセキュア情報が、少なくとも1つ以上“1”である場合、セキュア情報付き演算部222内のセキュア情報部223にはセキュア情報部210のセキュア情報“1”が伝搬し、セキュア情報付き演算部222が出力する演算結果のセキュア情報は保持される。

【0167】

また、被演算対象となる1つ以上のセキュア情報付き汎用レジスタ209のデータに付加されるセキュア情報部210のセキュア情報が、全て“0”である場合、セキュア情報付き演算部222内のセキュア情報部223にはセキュア情報付き命令デコーダ216内のセキュア情報部217のセキュア情報“1”が伝搬

し、セキュア情報付き演算部 222 が出力する演算結果のセキュア情報は保持される。

【0168】

また、ユーザメモリ空間 202 の演算命令がセキュア情報付き命令デコーダ 216 によりデコードされた結果を受け、セキュア情報付き汎用レジスタ 209 のデータがセキュア情報付き演算部 222 に受け渡され、セキュア情報付き演算部 222 は演算を開始する。

【0169】

このとき、被演算対象となる 1 つ以上のセキュア情報付き汎用レジスタ 209 のデータに付加されるセキュア情報部 210 のセキュア情報が、少なくとも 1 つ以上 “1” である場合、セキュア情報付き演算部 222 内のセキュア情報部 223 にはセキュア情報部 210 のセキュア情報 “1” が伝搬し、セキュア情報付き演算部 222 が出力する演算結果のセキュア情報は保持される。

【0170】

また、被演算対象となる 1 つ以上のセキュア情報付き汎用レジスタ 209 のデータに付加されるセキュア情報部 210 のセキュア情報が、全て “0” である場合、セキュア情報付き演算部 222 内のセキュア情報部 223 にはセキュア情報付き命令デコーダ 216 内のセキュア情報部 217 のセキュア情報 “0” が伝搬し、セキュア情報付き演算部 222 が出力する演算結果はセキュアでないという情報が付加される。

【0171】

セキュア情報付き演算部 222 のデータを外部空間 212 に転送する場合の動作は、実施の形態 6 において説明した内容と同様であるため、その説明を省略する。

【0172】

以上の構成により、セキュアメモリ空間の命令であり、かつ、演算を行う命令を実行する場合、被演算対象となる全データがユーザメモリ空間のデータであっても、またはセキュア情報部にセキュアデータであることが明示されていなくても、セキュアメモリ空間の命令に付加されるセキュア情報をセキュア情報付き演

算部のセキュア情報に反映することにより、演算結果が外部空間に流出することを防ぎ、例えば、演算結果からセキュアメモリ空間の命令内容を類推することを防御することができるという格別の効果を奏する。

【0173】

【発明の効果】

以上のように本発明によれば、ユーザメモリ空間から汎用レジスタにデータを転送した場合はセキュア情報部の値をセキュリティ不要状態とし、セキュアメモリ空間から汎用レジスタにデータを転送した場合はセキュア情報部の値をセキュリティ必要状態とし、セキュア情報部の値がセキュリティ必要状態である汎用レジスタからユーザメモリ空間へのデータ転送が禁止されるようにする制御を行うことによって、セキュアメモリ空間上の暗号鍵等のセキュアプログラム、セキュアデータが読まれることを防ぐことができる。

【0174】

同様に、特権モードと通常モードの切り替え制御を行わずして、セキュアメモリ空間から外部空間へのデータ転送を禁止することができる。さらに、セキュア情報付き内蔵RAM空間に対してもセキュア情報を追従させ、内蔵RAM空間を経由するデータのセキュリティ管理を可能とする。さらに、セキュアメモリ空間の割り込み退避データの読み出しによるハッキングを防御できる。さらに、ユーザメモリ空間の命令に許可されていないセキュアメモリ空間へのアクセスを制限できる。さらに、CPUが介在しないDMA転送データに対してもセキュア情報を追従させ、DMAを経由するデータのセキュリティ管理を可能とする。さらに、演算結果にもセキュア情報を追従させることにより外部空間への漏洩を防ぎ、セキュアメモリ空間の命令内容を類推することを防御することができる。

【0175】

すなわち、セキュア情報部を設けることで、従来のOSが行っていた特権モード、通常モードのモード切り替え制御を全て付加ビットにより代行し、かつ僅かなハード変更で事足りる、という利点がある。特に、PDAやデジタルテレビ等、コンテンツサービスにかかわる商品開発では有利な展開が期待される。

【図面の簡単な説明】

- 【図 1】 本発明の実施の形態 1 における情報処理装置の構成を示す概念図
- 【図 2】 本発明の実施の形態 1 における情報処理装置の動作を示すフローチャート
- 【図 3】 本発明の実施の形態 2 における情報処理装置の構成を示す概念図
- 【図 4】 本発明の実施の形態 2 における情報処理装置の動作を示すフローチャート
- 【図 5】 本発明の実施の形態 3 における情報処理装置の構成を示す概念図
- 【図 6】 本発明の実施の形態 3 における情報処理装置の動作を示すフローチャート
- 【図 7】 本発明の実施の形態 4 における情報処理装置の構成を示す概念図
- 【図 8】 本発明の実施の形態 4 における情報処理装置の動作を示すフローチャート
- 【図 9】 本発明の実施の形態 5 における情報処理装置の構成を示す概念図
- 【図 10】 本発明の実施の形態 5 における情報処理装置の動作を示すフローチャート
- 【図 11】 本発明の実施の形態 6 における情報処理装置の構成を示す概念図
- 【図 12】 本発明の実施の形態 6 ～ 10 におけるセキュア情報付き内蔵 RAM 空間、セキュア情報付き汎用レジスタの概念図
- 【図 13】 本発明の実施の形態 6 ～ 9 におけるセキュア情報付き内蔵 RAM 空間のアクセス状態図
- 【図 14】 本発明の実施の形態 7 における情報処理装置の構成を示す概念図
- 【図 15】 本発明の実施の形態 7, 8, 10 におけるセキュア情報付き命令デコーダ、セキュア情報付き割り込み退避情報部の概念図
- 【図 16】 本発明の実施の形態 8 における情報処理装置の構成を示す概念図
- 【図 17】 本発明の実施の形態 8 におけるセキュア情報付き内蔵 RAM 空間のスタック領域の状態図
- 【図 18】 本発明の実施の形態 9 における情報処理装置の構成を示す概念図
- 【図 19】 本発明の実施の形態 9 におけるセキュア情報付き DMA の概念図
- 【図 20】 本発明の実施の形態 10 における情報処理装置の構成を示す概念図

図

【図 21】 本発明の実施の形態 10 におけるセキュア情報付き演算部の概念

図

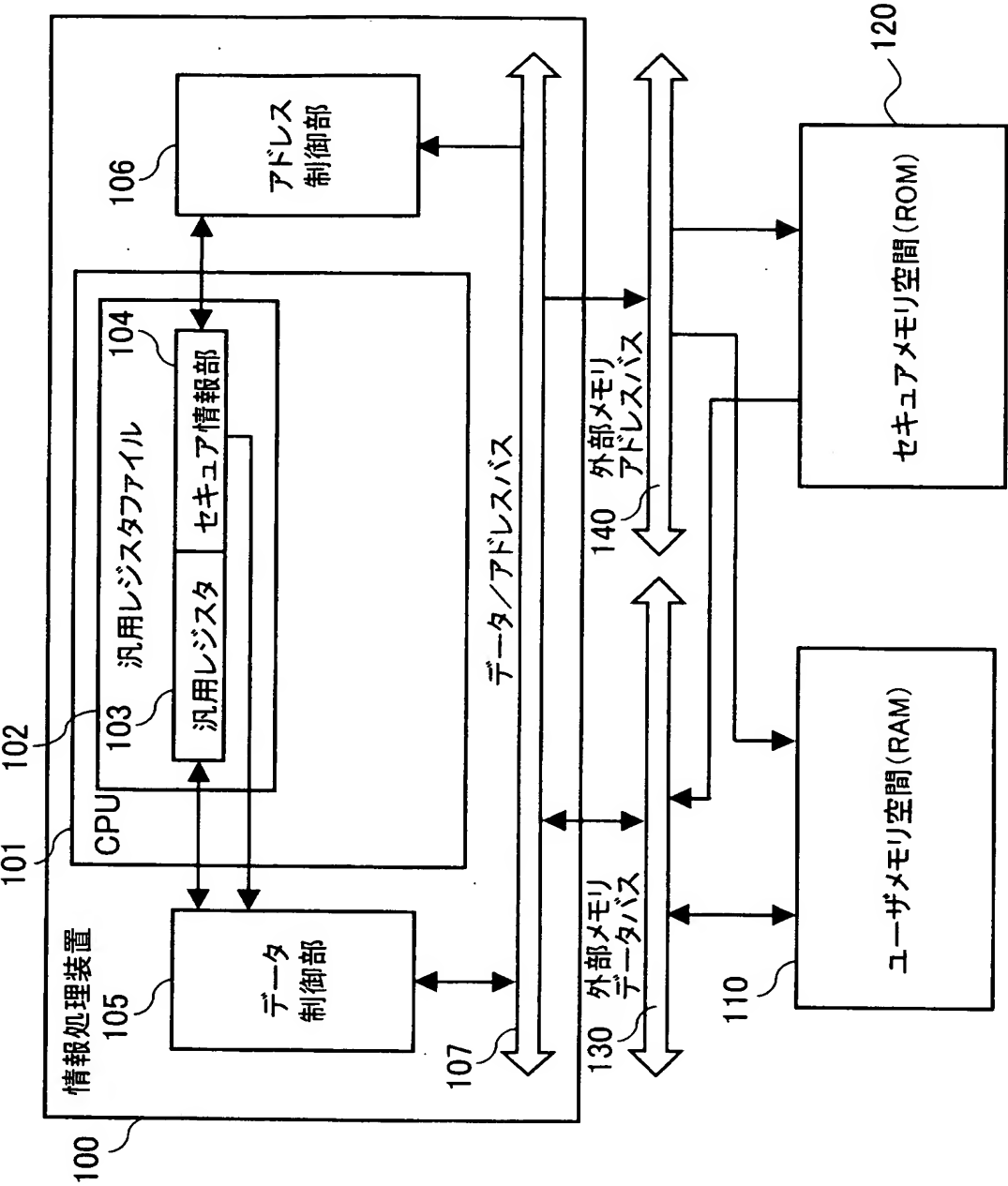
【符号の説明】

- 100 情報処理装置
- 101 CPU
- 102 汎用レジスタファイル
- 103 汎用レジスタ
- 104 セキュア情報部
- 105 データ制御部
- 106 アドレス制御部
- 107 データ／アドレスバス
- 108 命令フェッチアドレス制御部
- 109 命令バッファ
- 110 ユーザメモリ空間 (RAM)
- 110p ユーザプログラム
- 120 セキュアメモリ空間 (ROM)
- 120p セキュアプログラム
- 201 セキュアメモリ空間
- 202 ユーザメモリ空間
- 203 データバス
- 204 アドレスバス
- 205 セキュア情報生成部
- 206 セキュア情報付き内蔵 RAM 空間
- 207 セキュア情報付き内蔵 RAM 空間内のセキュア情報部
- 208 CPU
- 209 セキュア情報付き汎用レジスタ
- 210 セキュア情報付き汎用レジスタ内のセキュア情報部
- 211 データ出力制御部

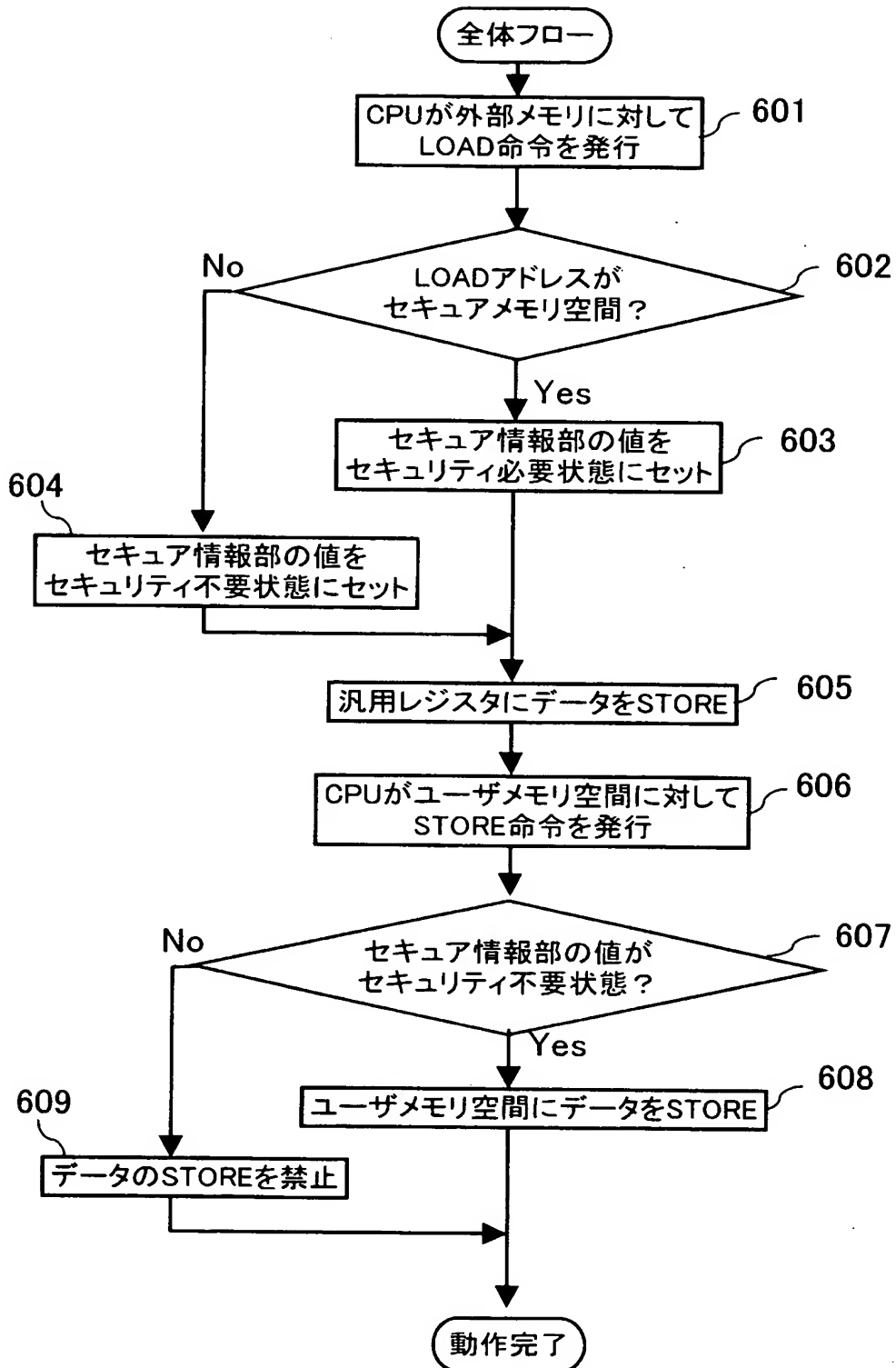
- 2 1 2 外部空間
- 2 1 3 割り込み制御部
- 2 1 4 セキュア情報付き割り込み退避情報部
- 2 1 5 セキュア情報付き割り込み退避情報部内のセキュア情報部
- 2 1 6 セキュア情報付き命令デコーダ
- 2 1 7 セキュア情報付き命令デコーダ内のセキュア情報部
- 2 1 8 スタックポインタ
- 2 1 9 退避情報書き換え制御部
- 2 2 0 セキュア情報付きDMA
- 2 2 1 セキュア情報付きDMA内のセキュア情報部
- 2 2 2 セキュア情報付き演算部
- 2 2 3 セキュア情報付き演算部内のセキュア情報部
- 3 0 0 第1の汎用レジスタ
- 3 0 1 第2の汎用レジスタ
- 3 0 2 第3の汎用レジスタ
- 3 0 3 第1のセキュア情報部
- 3 0 4 第2のセキュア情報部
- 3 0 5 第3のセキュア情報部
- 4 0 0 状態レジスタ
- 5 0 0 端末P C
- 5 0 1 ユーザI O空間 (R A M)
- 5 0 2 セキュアI O空間 (R A M)
- 5 0 3 I Cカード
- S 5 0 3 デバッグ鍵
- 7 0 3 c スタック退避情報

【書類名】 図面

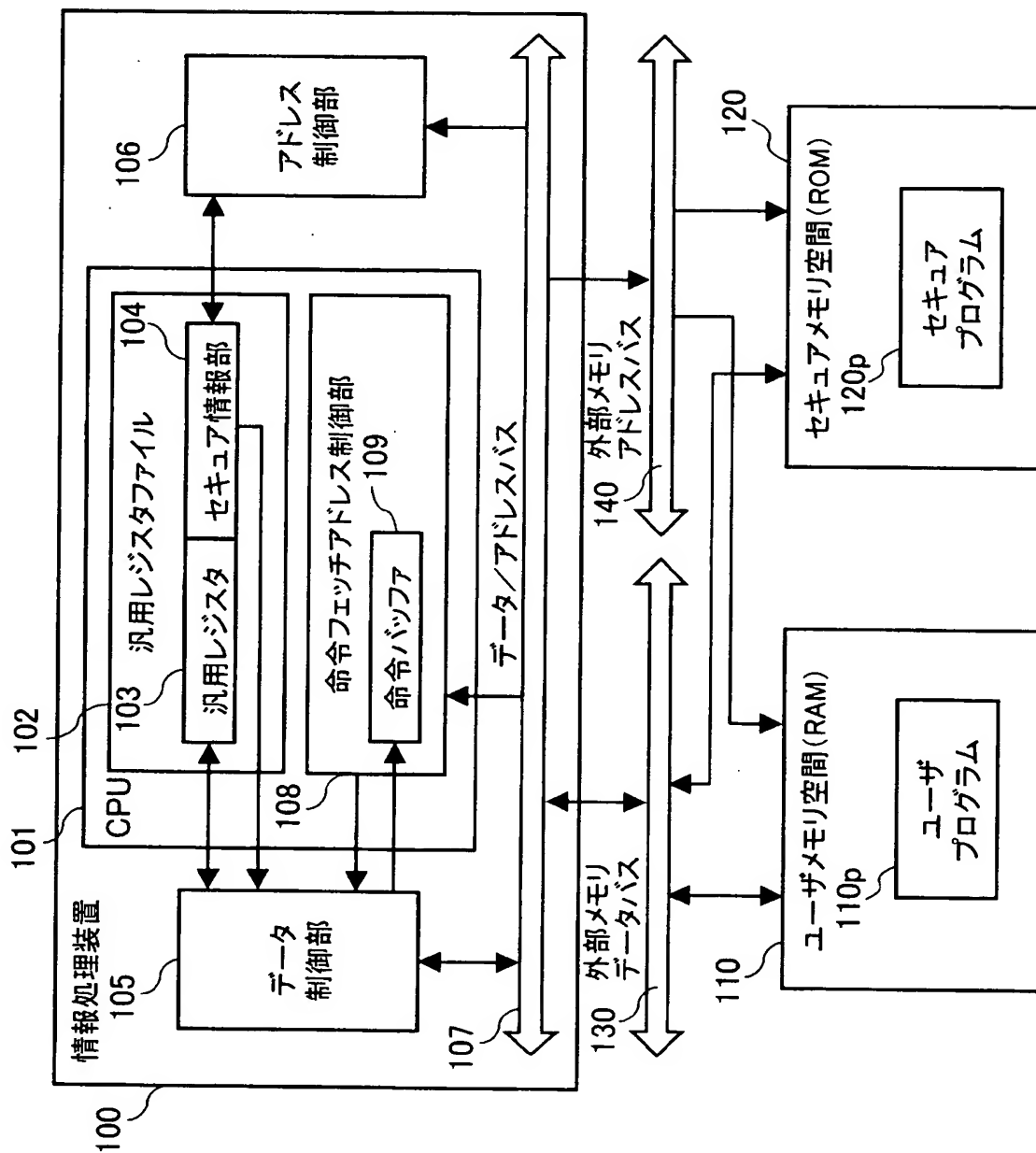
【図 1】



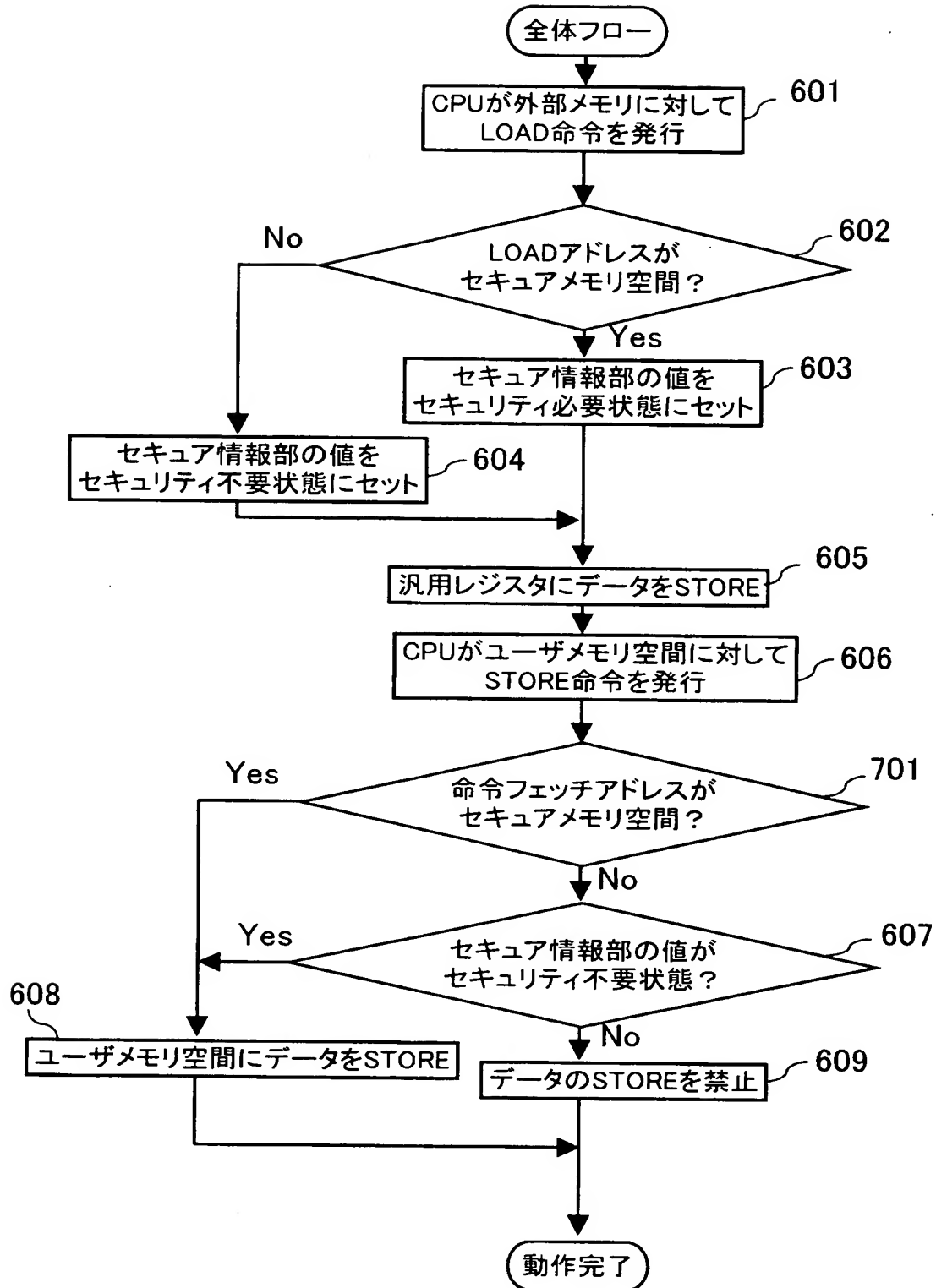
【図 2】



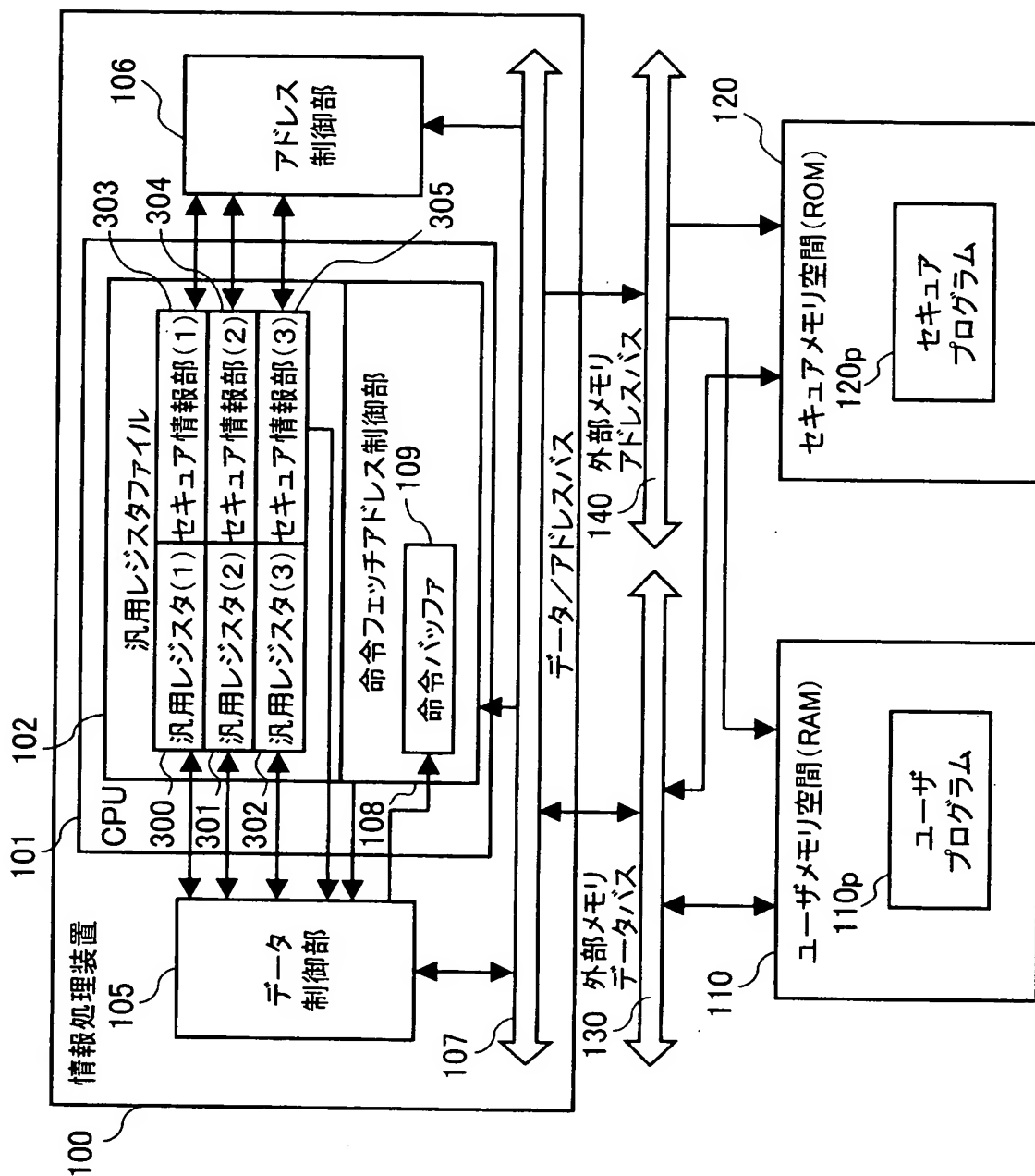
【図 3】



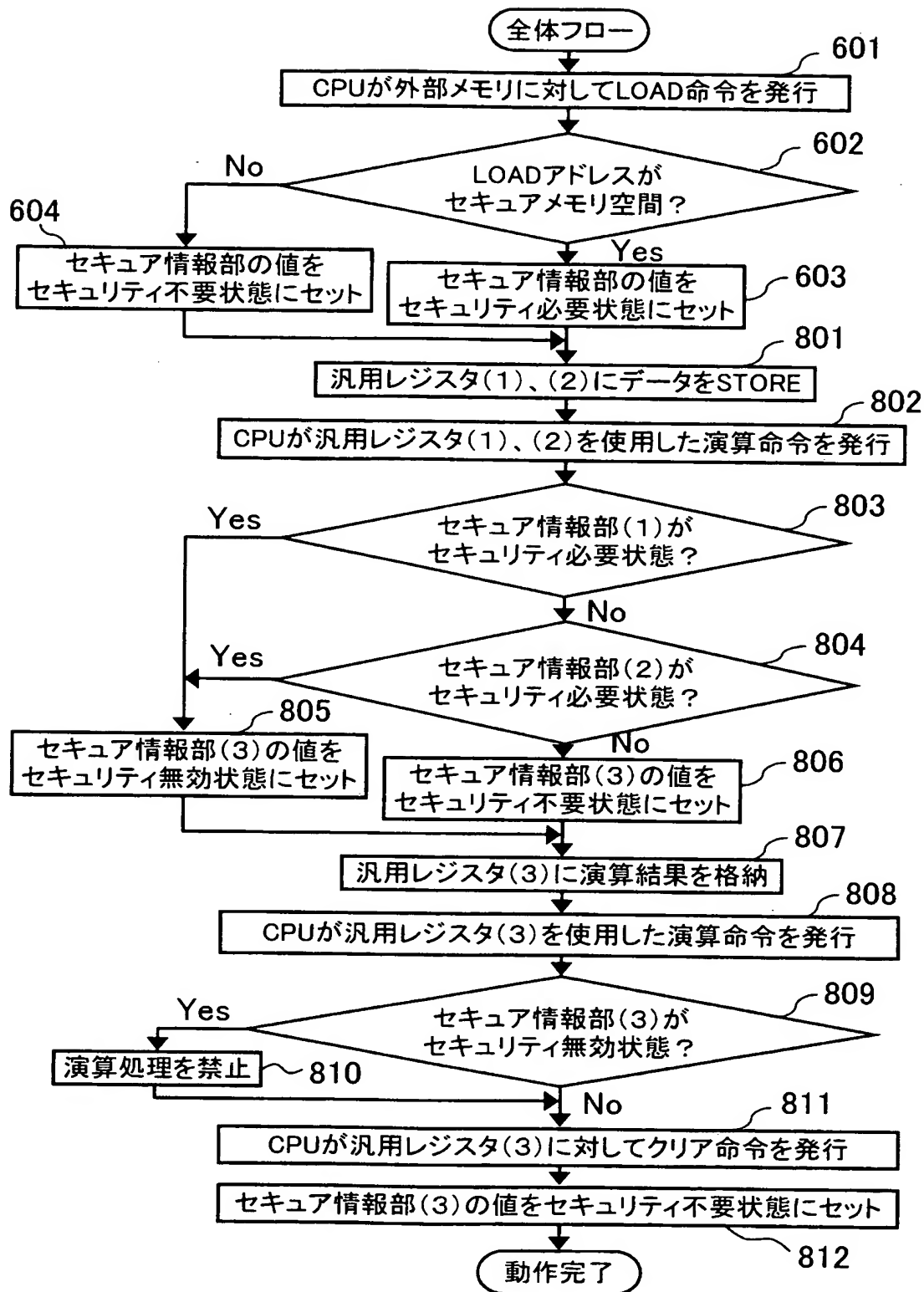
【図 4】



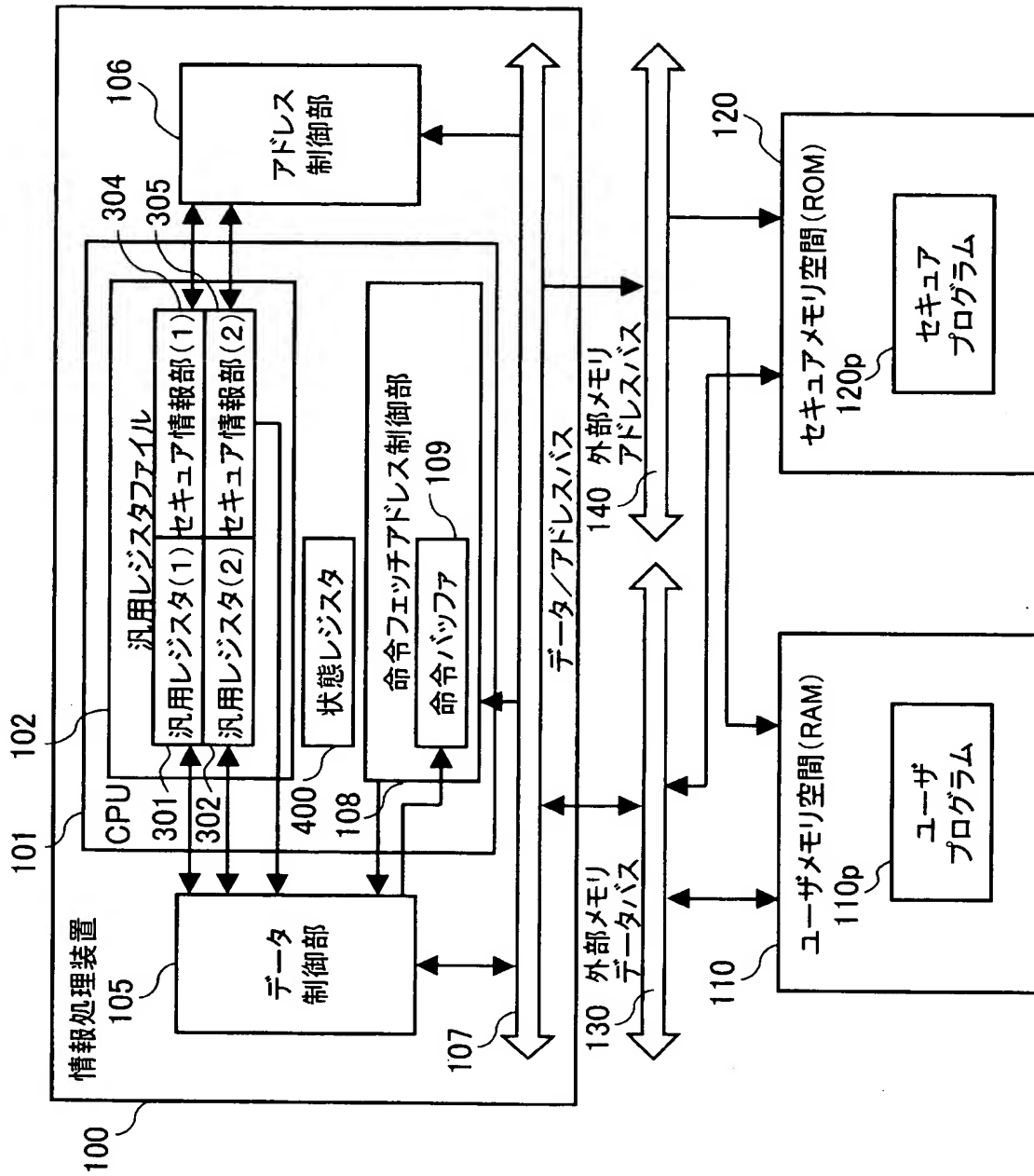
【図 5】



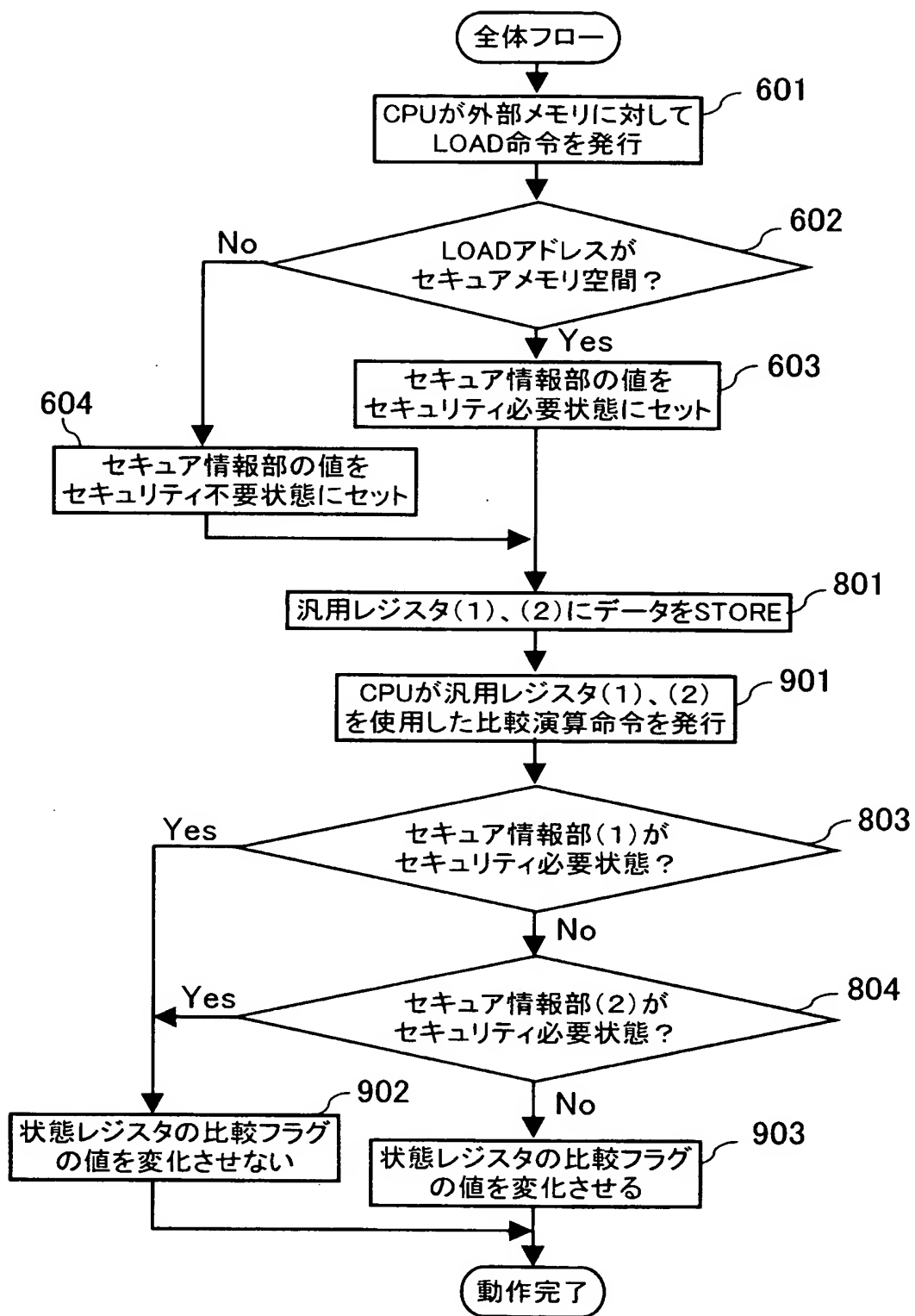
【図 6】



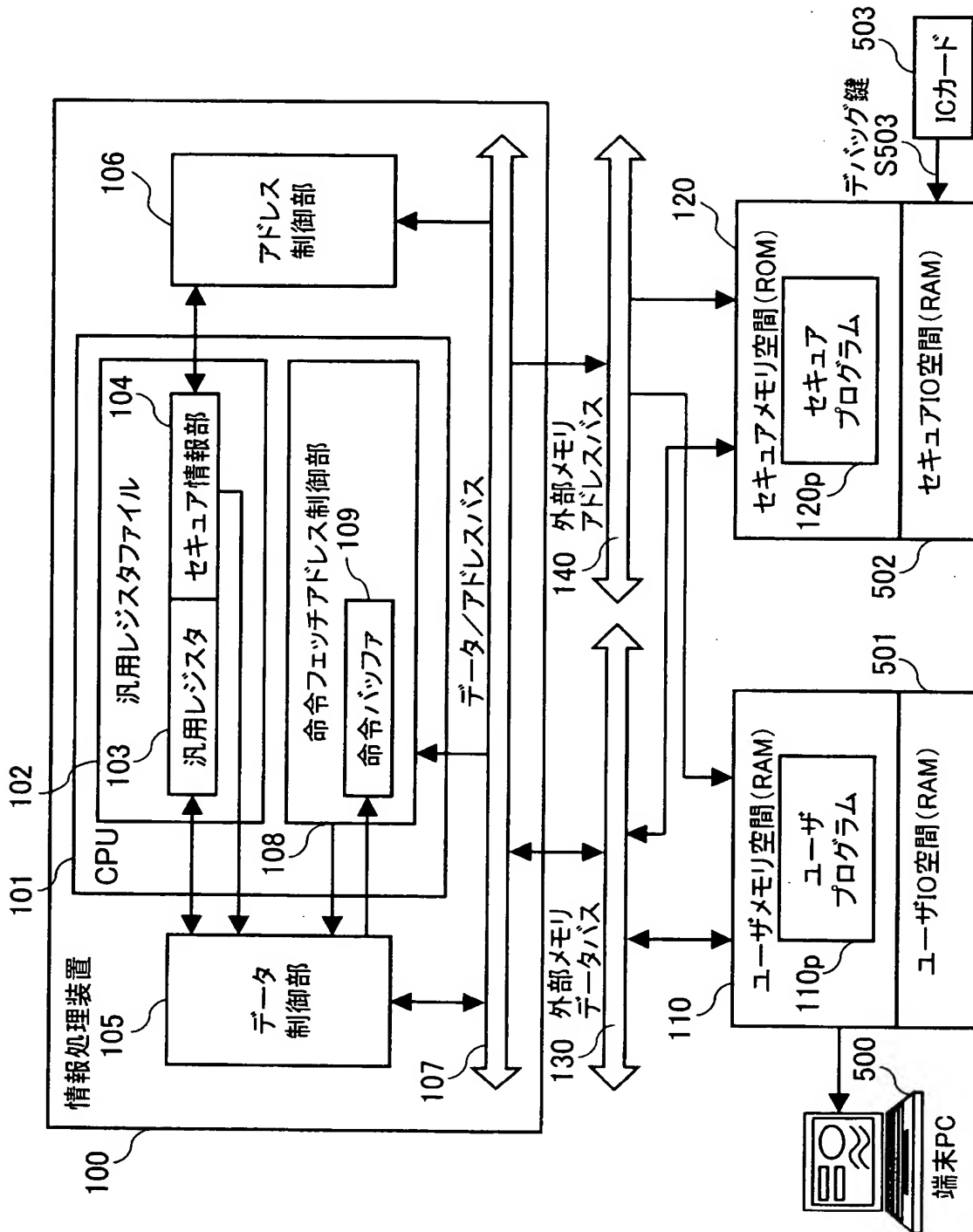
【図 7】



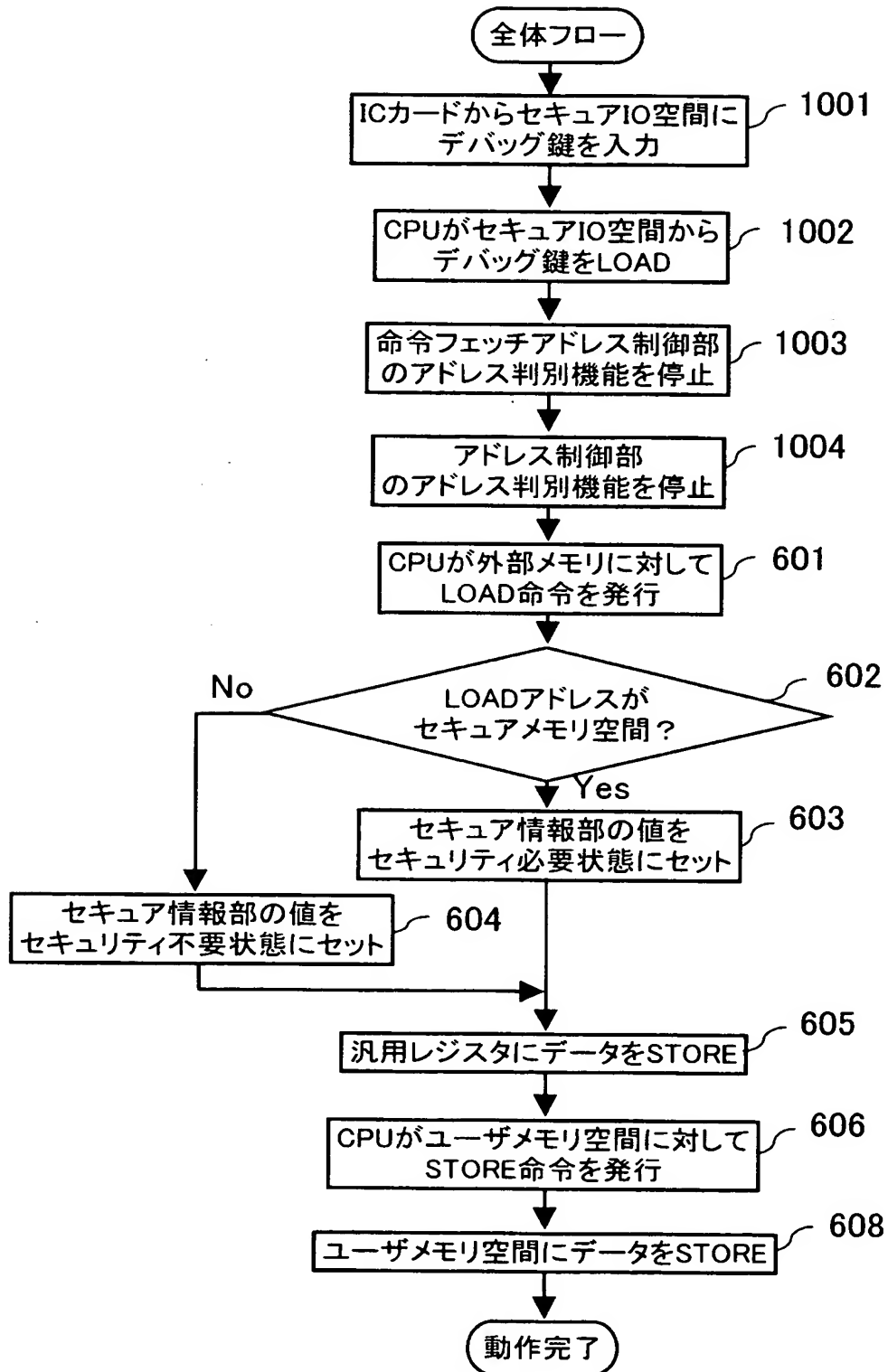
【図 8】



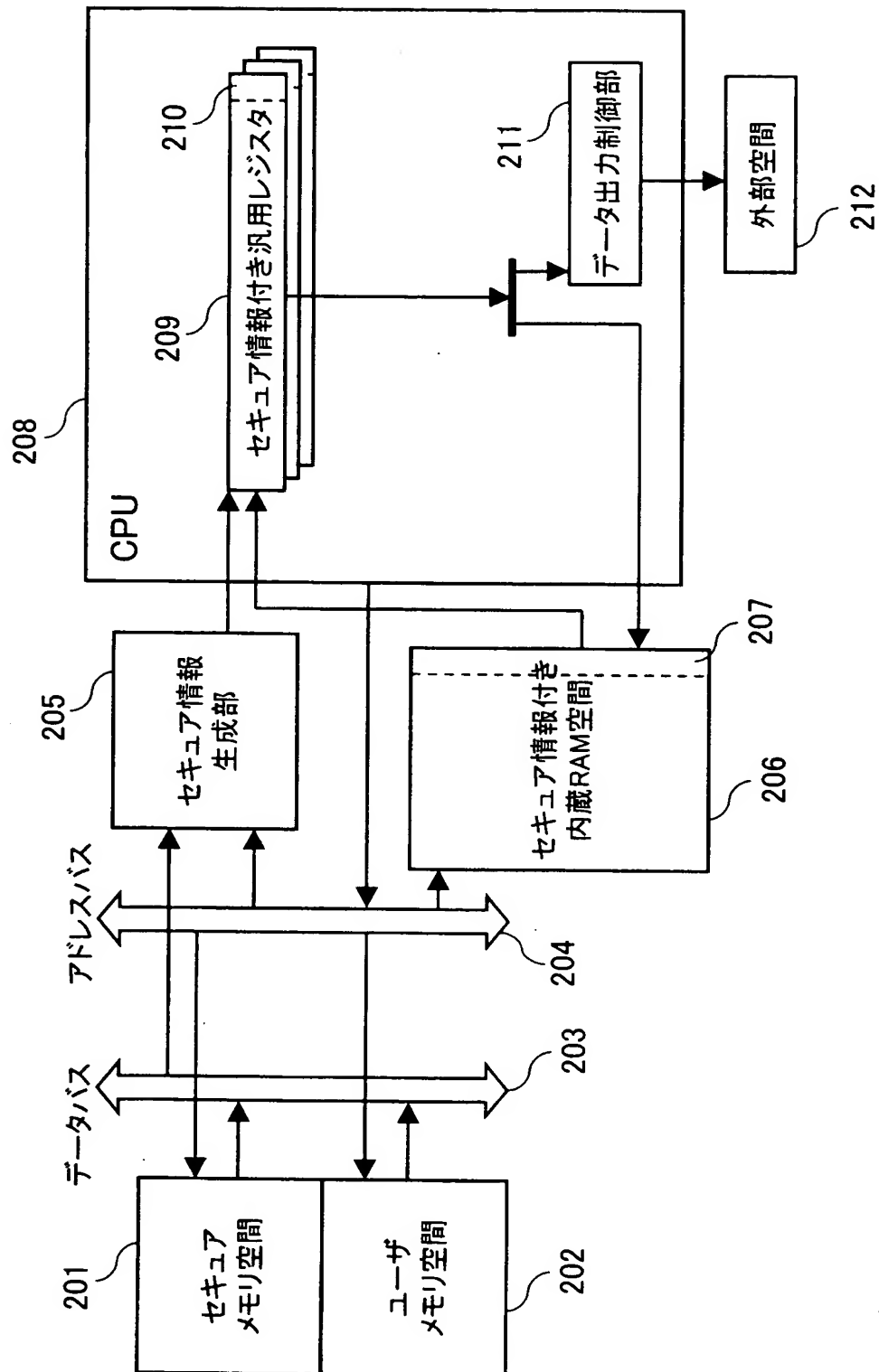
【図9】



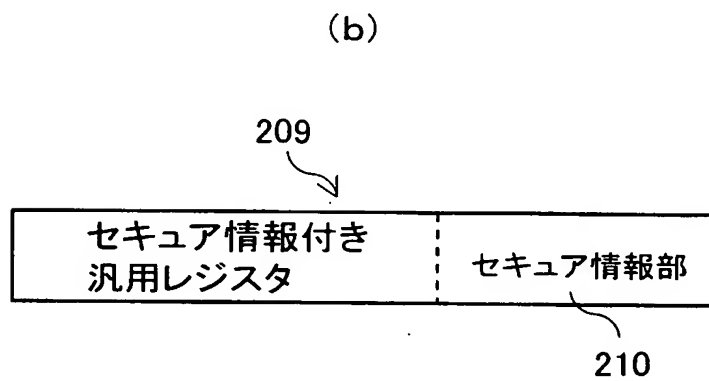
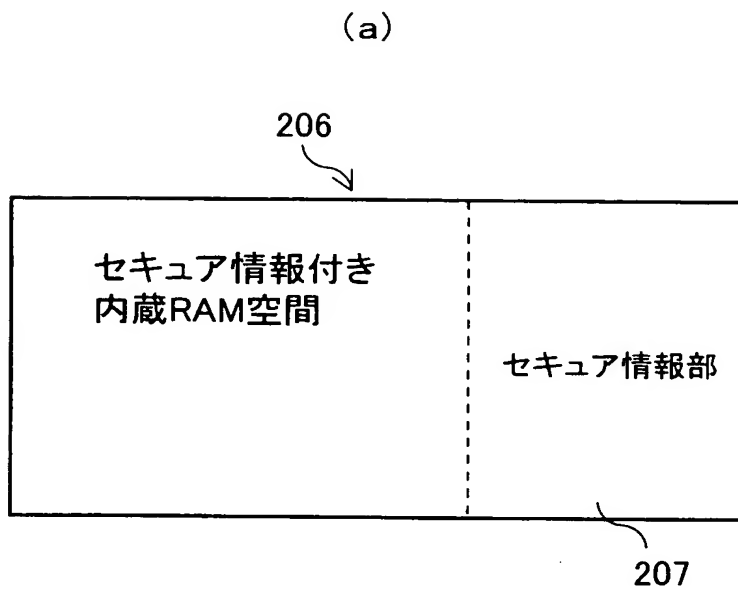
【図10】



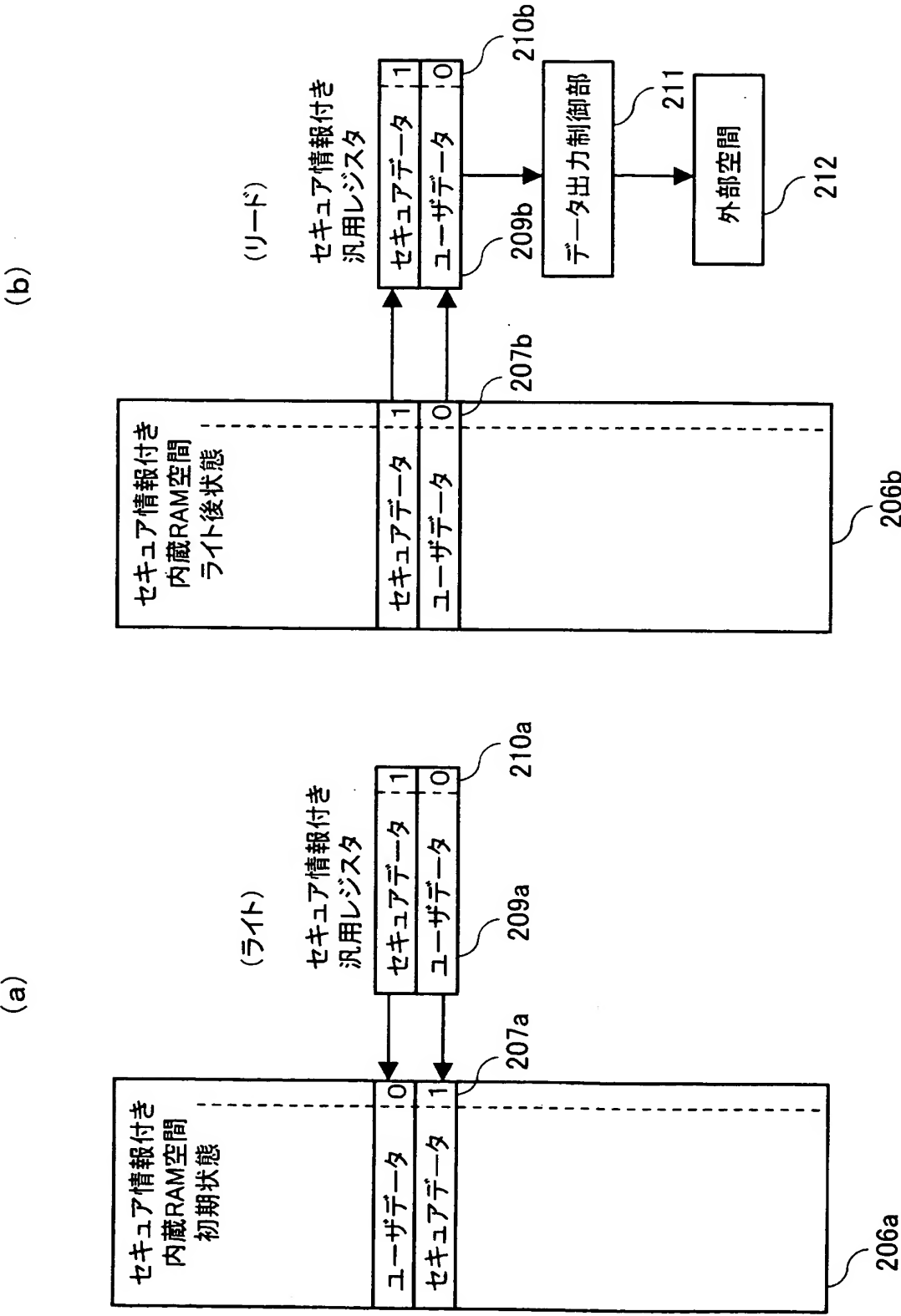
【図 11】



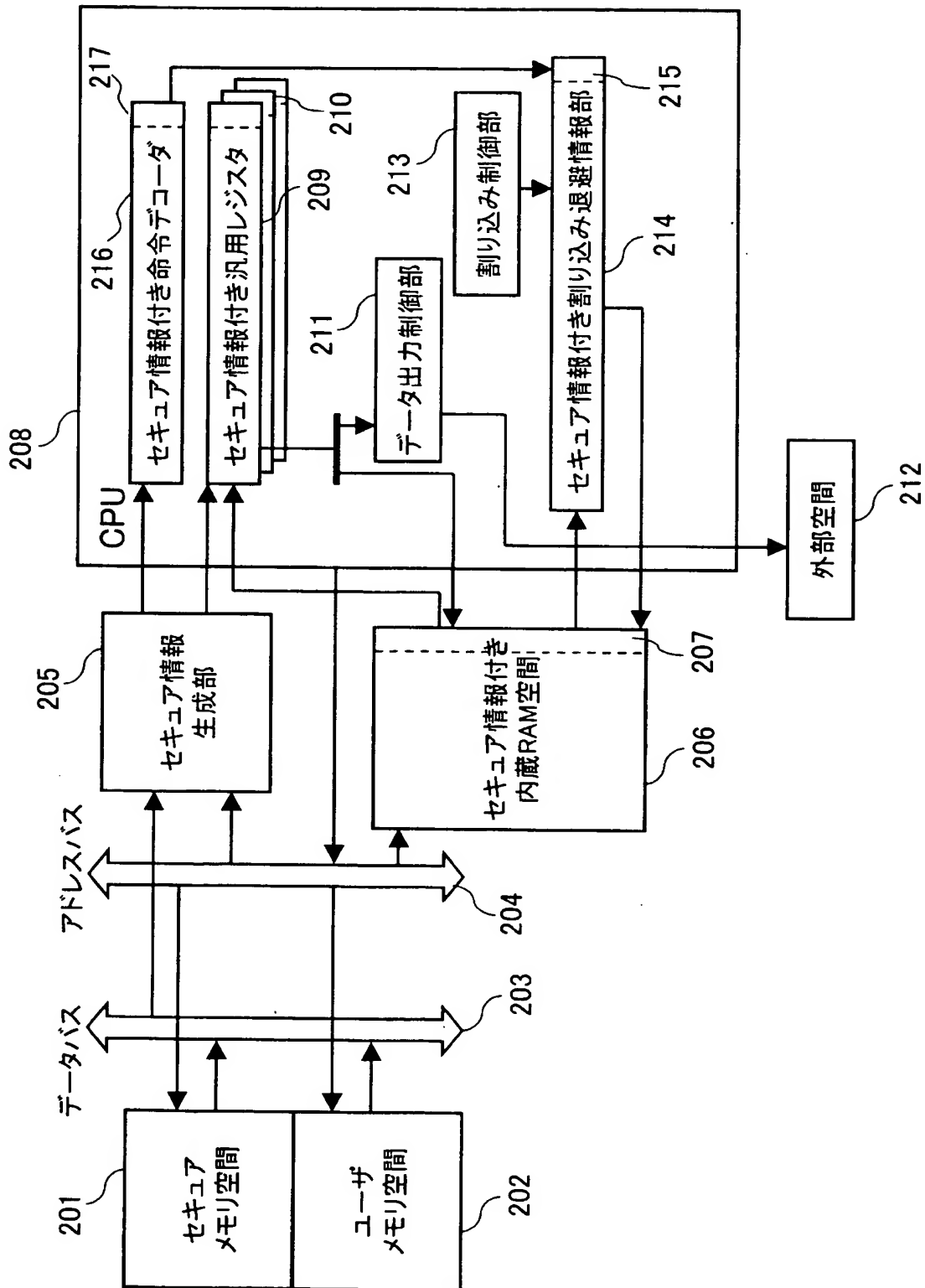
【図 12】



【図 13】

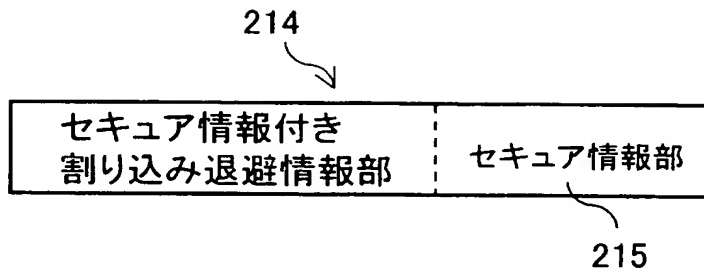


【図 14】

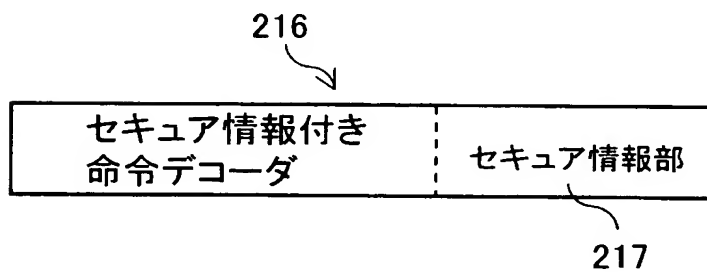


【図 15】

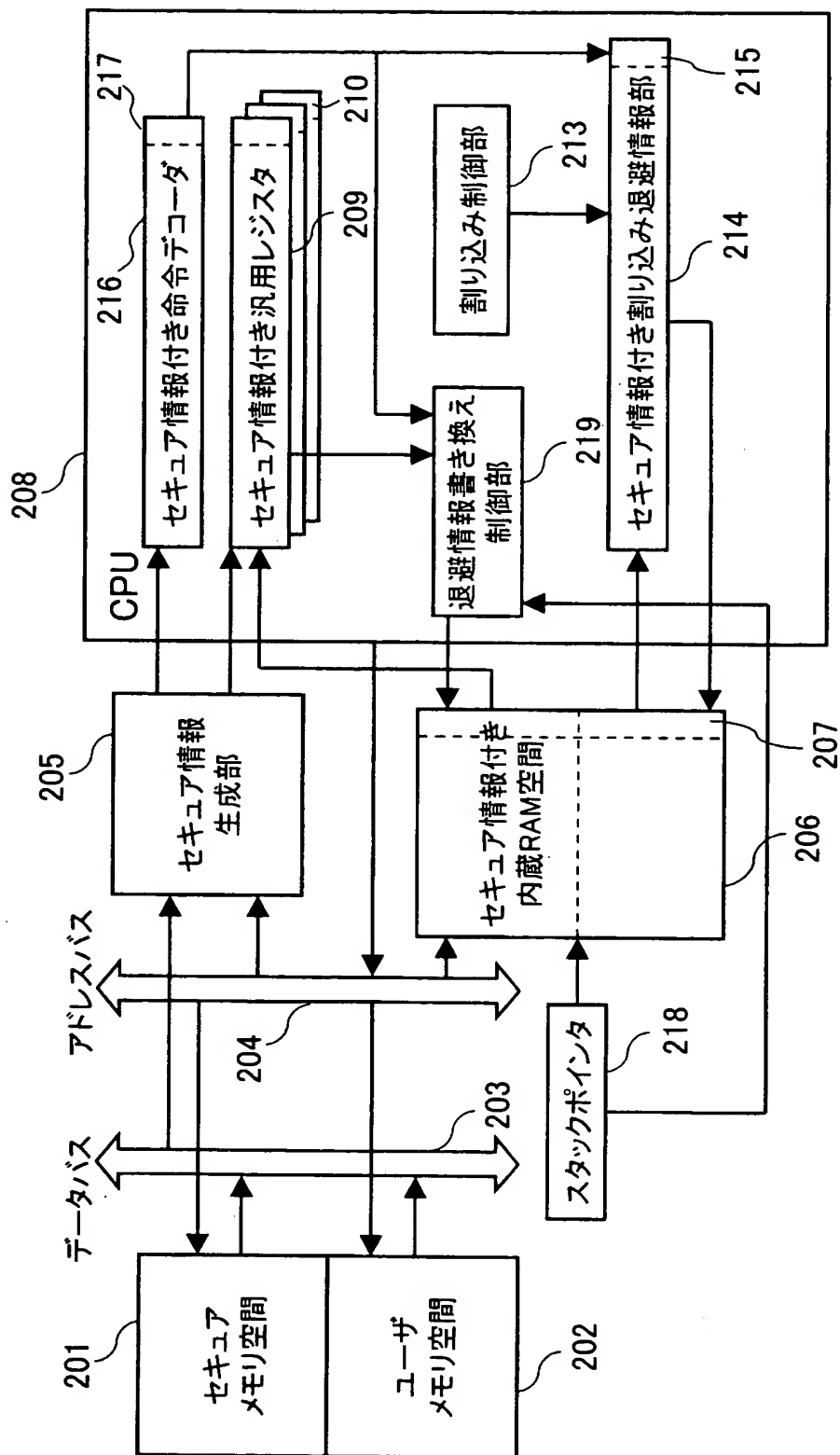
(a)



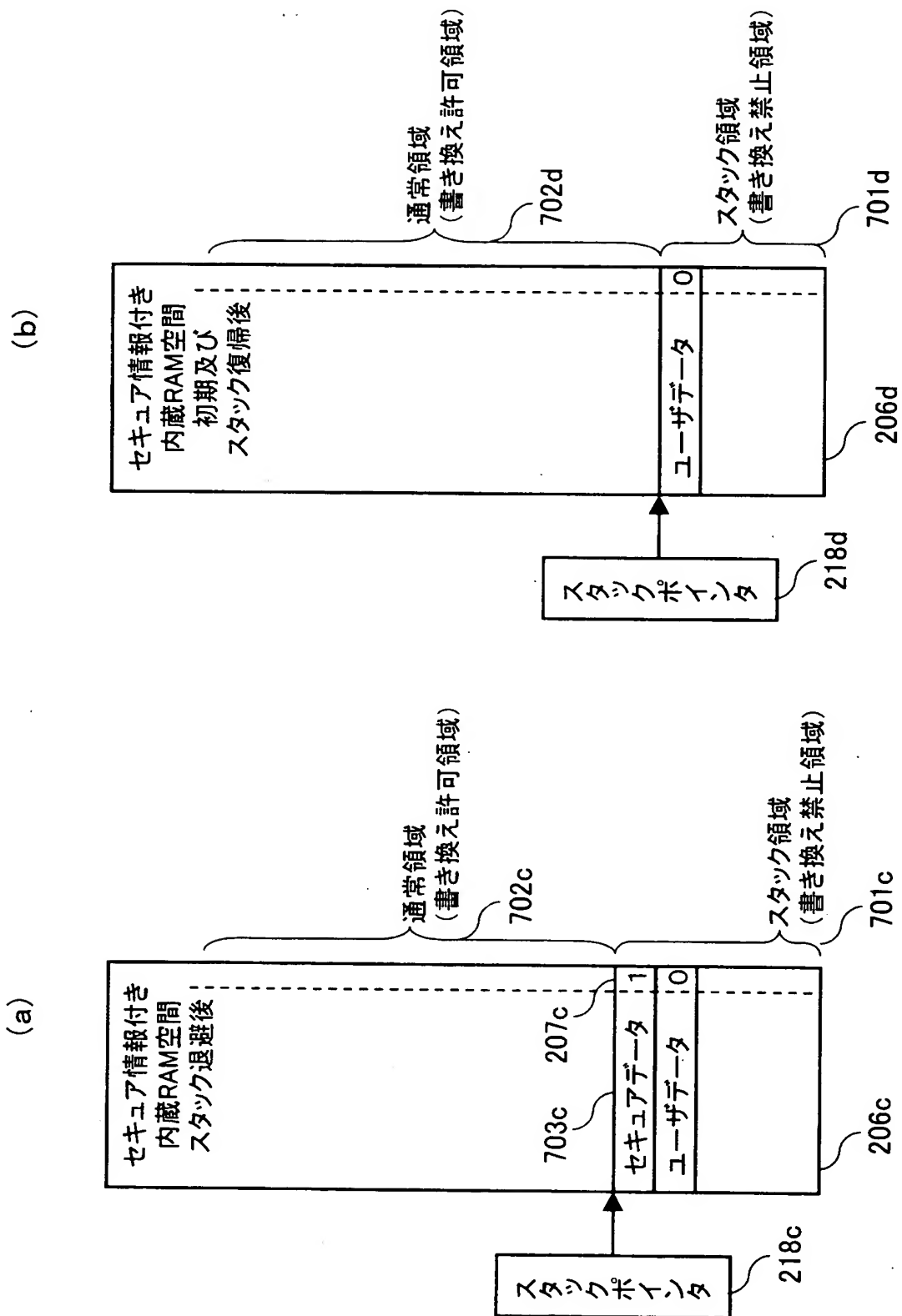
(b)



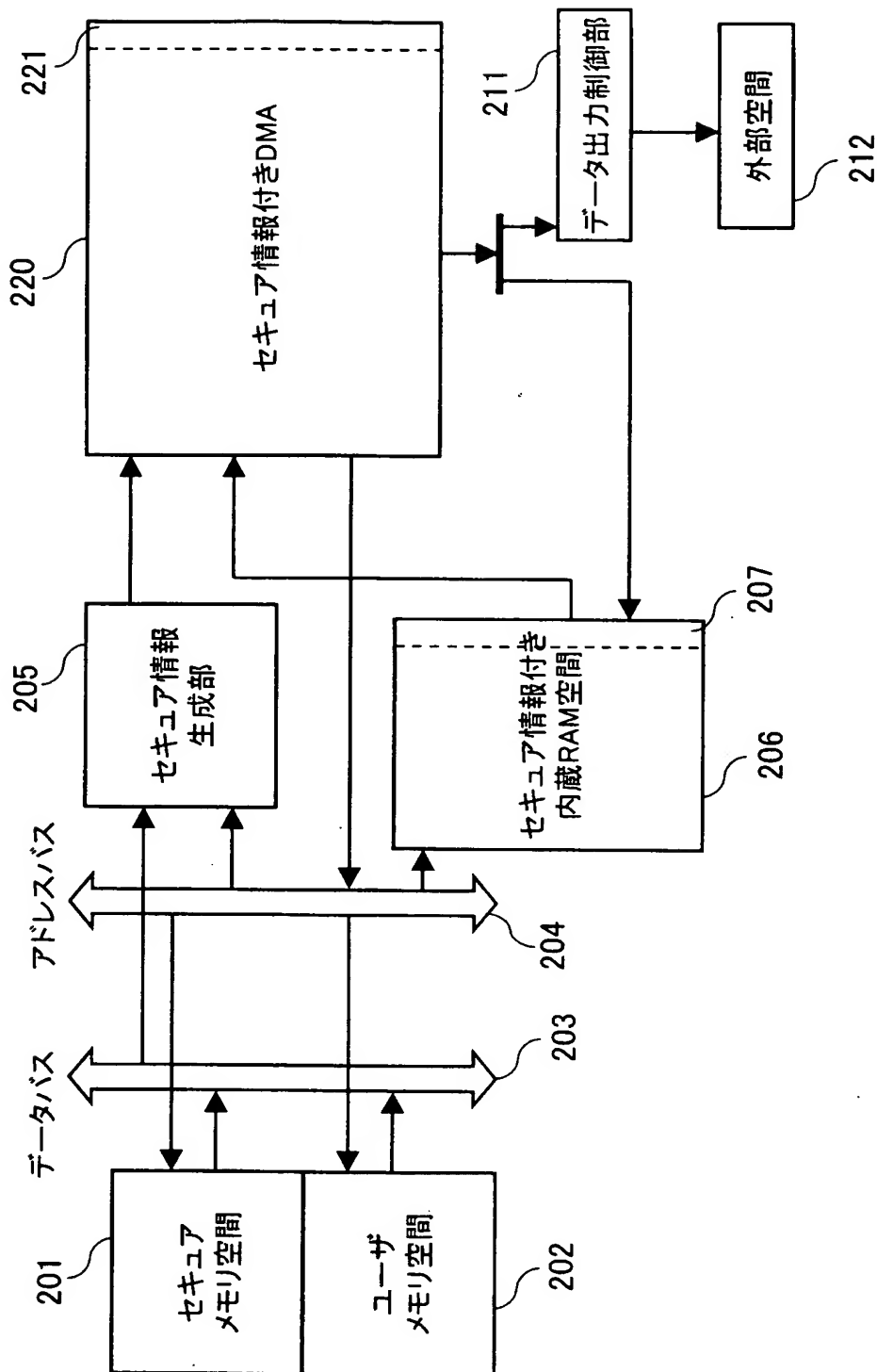
【図 16】



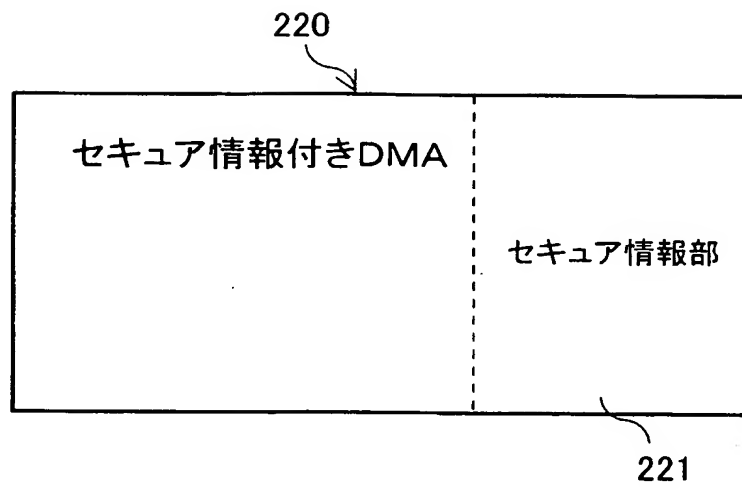
【図17】



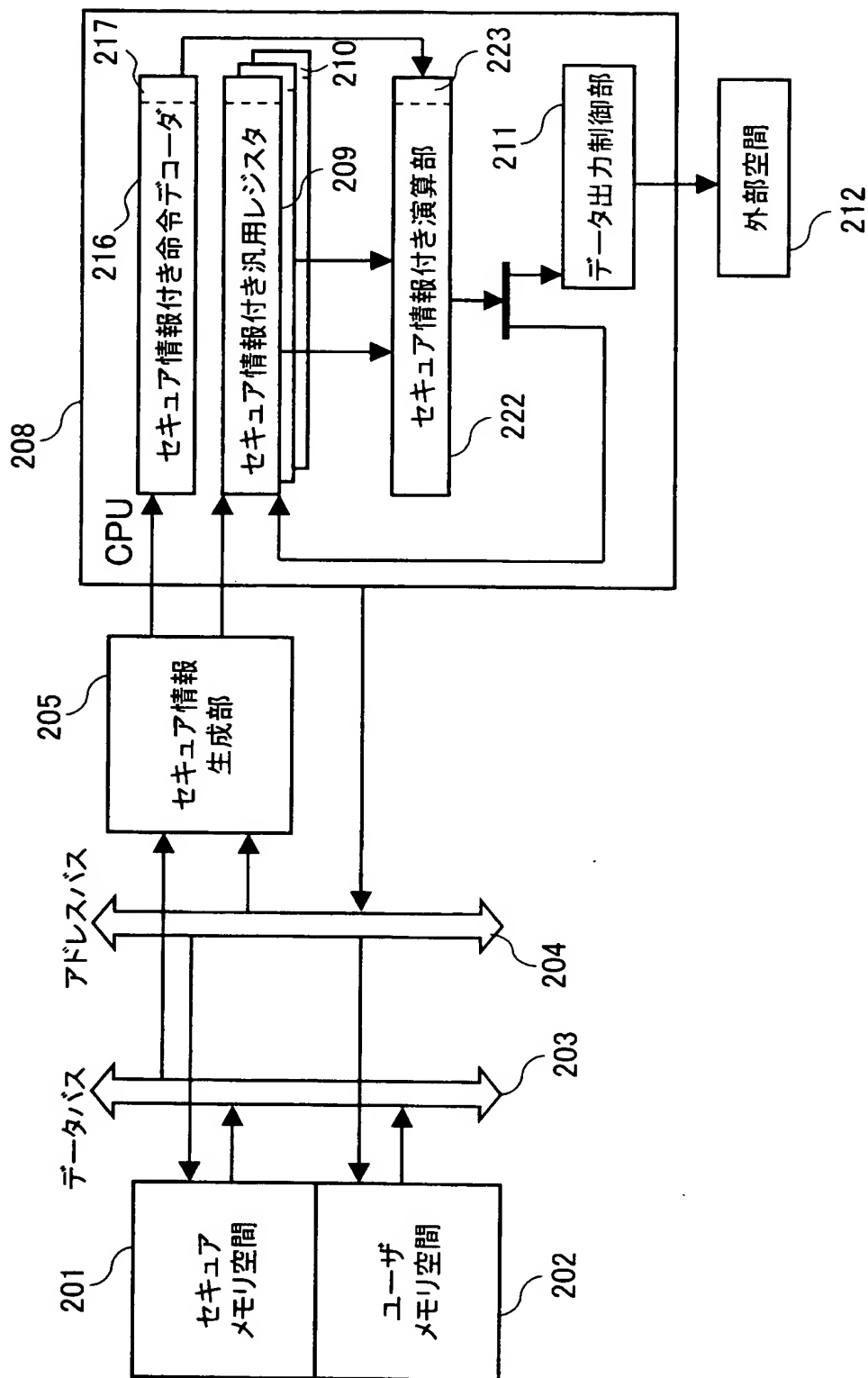
【図 18】



【図 19】

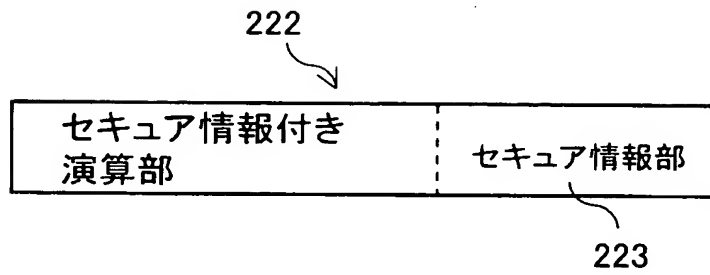


【図 20】





【図 21】





【書類名】 要約書

【要約】

【課題】 従来の特権モードによるメモリ保護ではなく、セキュアメモリ空間のデータや命令を外部に読み出すことをできなくし、従来技術で行われる悪用を回避する。

【解決手段】 ユーザメモリ空間 110 から汎用レジスタ 103 にデータを転送した場合はセキュア情報部 104 の値をセキュリティ不要状態とし、セキュアメモリ空間 120 から汎用レジスタ 103 にデータを転送した場合はセキュア情報部 104 の値をセキュリティ必要状態とし、セキュア情報部 104 の値がセキュリティ必要状態である汎用レジスタ 103 からユーザメモリ空間 110 へのデータ転送が禁止されるようにする制御を行うことによって、セキュアメモリ空間 120 上の暗号鍵が読まれることを防ぐ。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 2 6 8 1 0
受付番号	5 0 3 0 0 1 7 4 5 0 8
書類名	特許願
担当官	第二担当上席 0 0 9 1
作成日	平成 1 5 年 2 月 1 4 日

< 認定情報・付加情報 >

【提出日】 平成 15 年 2 月 4 日

次頁無

特願 2 0 0 3 - 0 2 6 8 1 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日
[変更理由]

1 9 9 0 年 8 月 2 8 日
新規登録

住 所
氏 名

大阪府門真市大字門真 1 0 0 6 番地
松下電器産業株式会社